stryker
Form

Document Title	Product security Standard Assessment
Document number / Revision	D001020014 / 01
Date	8-Apr-22
Project	SmartMedic Phase II
Project number	SGTC-NPD-001

Approvals

Approvals	Name	Title	Signature	Date
Author	Deepak Sharma	Design Engineering R&D (Software)		
Approvers	Pragya Nidhi	Test Engineering		
	Vikram Puri	Advanced Operations (Mfg & QA)		
	Sreejith Viswam	Advance Quality Engineer		

PRODUCT SECURITY STANDARD ASSESSMENT - Header

Section 1. Identifying Information (enter N/A for any items that do not apply)			
Document Number	D001020014	**Author**	Deepak Sharma
Document Revision	01	**Project Lead**	Akhil Gupta
Project Name	SmartMedic Phase II	**Division/Function**	NPD
Project (DHF) Number	SGTC-NPD-000-02	**Business Unit**	R&D
Description of Medical Device/System in scope	SmartMedic -001-02-A-00-00-00 SmartMedic is an AC powered (with AC to DC adaptor) device intended for use on Hospital Beds. It is designed to provide improved patient care in the hospital facility. The device is secured in place on top of the bed frame and under the bed's mattress. The device can provide patient weight, turn indication and share information with authorized hospital nurse station. The system shares and displays information on hospital's Nurse station through cloud application. The device also supports functionality for placing x-ray cassette without moving the patient on bed.	**Comments**	

Change History (Rows may be added)

Revision	Comment	Date	Author
00	Initial Release DR1-4 Document was reviewed but not approved and archived, thus archiving	30-Aug-21	Deepak Sharma
01	-Document updated as per DR5-7 requirement - SmartMedic Part number corrected (Typo error) in Header Tab: Description of Medical Device/System in scope -"Rationale for not using Traceability reference if using" updated in sheet Capabilities Assessment Sheet-"Traceability Reference" updated in sheet Security Controls Assessment -"Traceability Reference" updated in Sheet Privacy Controls Assessment	8-Apr-22	Deepak Sharma

Form Instructions

1. Complete Identifying Information (Section 1). Keep information up to date if document in revised. Use of Change History section is optional unless required by local procedure.
   Note: The Table of Contents below explains the purpose of each worksheet in this file. Only the first three worksheets must be completed. The others are for reference.
2. Complete the Capabilities Assessment worksheet, following instructions on that page.
3. Complete the Security Controls Assessment worksheet, following instructions on that page.
4. Complete the Privacy Controls Assessment worksheet, if required.
5. Refer to D0000061606 for requirements concerning when and how this PSSA is to be used in the overall software design process.

Table of Contents

Worksheet	Explanation	Form/Reference
Header	Document information, product identification, revision history	Form
Capabilities Assessment	Form on which to select security level, relevant capabilities, and whether privacy by design elements are relevant	Form
Security Controls Assessment	Form on which to select applicable security controls, or to justify not implementing them in the design	Form
Privacy Controls Assessment	Form on which to select applicable privacy controls, or to justify not implementing them in the design	Form
Logic Tables	Formula tables used to determine which controls and control enhancements must be assessed based on selected standard, selected capabilities, and security level	*Reference*
Impact Levels	Guidance for selecting Potential Impact	*Reference*
Capabilities and MDS2	Chart listing the explanations of each security capability, and the MDS2 questions that correspond to each	*Reference*
Controls and Guidance	Details concerning the NIST security controls, including additional guidance, control enhancements, and Stryker-specific guidelines	*Reference*
Privacy BR	Full text of the Privacy by Design baseline requirements associated with each family and sub-element of the Privacy by Design framework	*Reference*

PRODUCT SECURITY STANDARD ASSESSMENT - Capabilities Assessment

DHF Reference:	SGTC-NPD-000-02
Product/Entity:	**SmartMedic -001-02-A-00-00-00** **SmartMedic is an AC powered (with AC to DC adaptor) device intended for use on Hospital Beds. It is designed to provide improved patient care in the hospital facility. The device is secured in place on top of the bed frame and under the bed's mattress. The device can provide patient weight, turn indication and share information with authorized hospital nurse station. The system shares and displays information on hospital's Nurse station through cloud application. The device also supports functionality for placing x-ray cassette without moving the patient on bed.**

Instructions for this worksheet

1. Refer to D0000061606 for requirements related to the PSSA.
2. Complete Section 2, selecting potential impact and entering rationale.
3. Select Yes/No for to indicate applicability of each capability listed in Section 3.
4. Enter rationale for any capability determined not to apply.
5. Complete Section 4 to determine if Privacy by Design requirements apply.
6. Proceed to complete the Security Controls Assessment worksheet.
7. For each applicable capability, once the capability has been added to the design inputs for the product, enter traceability reference number (e.g. the design inputs document number).

Section 2. Potential Impact Selection (See Impact Levels tab)

Category	Rationale for Selection	Selection
Confidentiality	Patient data is not stored in system. Identification of patient is not possible.	Low
Integrity	Limited impact even if the weight data is modified by unauthorized user. Only impacted system will be Nurse Station and any c	Low
Availability	Limited impact even if the weight or position data is not available on Nurse Station or the external system. To be included in SC	Low
	OVERALL Potential Impact Level	**Low**

Section 3. Applicable Security Capabilities

See AAMI/IEC TIR80001-2-8:2016 for relationship of each capability to NIST security controls. Click the Capability name to see additional explanation and a list of related MDS2 questions.

ID	Capability	Requirement Overview	Applicable?	Rationale for not using / Traceability reference if using
10	AUTOMATIC LOGOFF (ALOF)	System shall provide automatic logoff after a period of inactivity	Yes	SRS D001020097 - 2.1.2.5 -- The Application shall allow the user to be logged out if the session has ended or after 8 minutes of inactivity.
20	AUDIT CONTROLS (AUDT)	System shall provide audit controls documenting who is doing what with health data	Yes	SRS D001020097 - 2.23.2 - Audit logs
30	AUTHORIZATION (AUTH)	The system shall provide role based controlled access to health data and functions - access to be provided only as necessary to perform the tasks required consistent with intended use	No	SRS Item (Appicable to NurseStation, Tablet Application) : Single Access with hospital code. No need of authorization
40	CONFIGURATION OF SECURITY FEATURES (CNFS)	System shall provide the Hospital system administrator the ability to configure the products security capabilities	No	Relevant Security controls for the NurseStation and the Tablet Application are identifeid within this document. Any controls which may be relevant for any customer (and hospital IT) and which are beyond the trurst boundaries of the Stryker system will be adressed in the SOM (Security Operations Manual - D001020115)
50	CYBER SECURITY PRODUCT UPGRADES (CSUP)	The system shall provide the ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches	Yes	D001020115: Security Operations Manual -19. Cyber Security Product Upgrades : For tablet, the product upgrade shall be provided in the form of Application installer files and will be done by Stryker Service person. Nurse station is a web application which can be taken care by the server admin.
60	HEALTH DATA DE-IDENTIFICATION (DIDT)	The system shall provide the ability to directly remove information that allows identification of a person	Yes	SRS D001020023 - 2.13.2 - System shall store patient id in anonymized fashion.
70	DATA BACKUP AND DISASTER RECOVERY (DTBK)	The system shall have an integral data backup capability to recover after damage or destruction of device data, hardware or software	Yes	SRS D001020097 - 2.19.1 - The System shall use backup mechanism provided by Azure.
80	EMERGENCY ACCESS (EMRG)	The system shall provide users the ability to access private data in case of an emergency that requires immediate access to private data	No	The Intended Use does not requires this arrangement for private access
90	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)	The device shall ensure the integrity of stored data with implicit/explicit error detection/correction technology	No	NoPHI (personal health information) stored
100	MALWARE DETECTION/PROTECTION (MLDP)	The system shall support the use of anti-malware mechanism	Yes	SRS D001020024 -2.17.6 The Application shall support the use of anti-malware mechanism D001020115: Security Operations Manual- 23. Malware Detection/Protection SYK donot have control over the user desktop for Nursing application.
110	NODE AUTHENTICATION (NAUT)	The system shall provide node authentication to ensure that only known devices can connect with each other and share data	Yes	SRS D001020024 - 2.17.8 - Only Stryker made/ authenticated devices should be able to communicate with SM device and tablet. Bluetooth Authentication on device, DeviceID act as the key for device authentication Tablet provisioning on IOT Hub with tokens (Applicable to SmartMedic device, Tablet and Cloud connections)
120	PERSON AUTHENTICATION (PAUT)	The system shall provide the ability to authenticate users	Yes	SRS D001020024 - 2.17.3 :The application shall provide access to authorized users using authentication code D001020115: Security Operations Manual - 4. User Account Management Nurse station has authentication provided by entering hospital id. Additionaly application has the configuration options to monitor inactivity.
130	PHYSICAL LOCKS (PLOK)	The system components that maintain private data shall be physically secure	Yes	Applicable to Tablet- Physical enclosure to secure the tablet. D001020115: Security Operations Manual - 27. Physical Locks
140	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)	The system software development plan shall address security support of 3rd party components throughout system life cycle	Yes	Software Development Plan : D001020020 Applicable to SmartMedic Device, Tablet Application and Nurse Station application D001020115: Security Operations Manual - 24. Roadmap for Third Party Components in Device Life Cycle
150	SYSTEM AND APPLICATION HARDENING (SAHD)	System shall provide hardening features to guard against cyber attacks and malware	Yes	D001020115: Security Operations Manual - 26. System and Application Hardening D001020037 Penetration Testing Protocol reference for application hardening Applicable to Tablet Application.
160	SECURITY GUIDANCE (SGUD)	The system service/user manuals shall provide security guidance for operators and administrators	Yes	D001020115: Security Operations Manual Applicable to SmartMedic Device (Bluetooth and wifi connection), Tablet Application, Nurse Station and Hospital's WiFi network.
170	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)	The system shall establish technical controls to mitigate the potential for compromise to the integrity and confidentiality of health data stored on product or removable media	Yes	SRS D001020023 - 2.13.2 - System shall store patient id in anonymized fashion. D001020115: Security Operations Manual - 25. Health Data Storage Confidentiality
180	TRANSMISSION CONFIDENTIALITY (TXCF)	The system shall ensure confidentiality of transmitted health data	Yes	D001020115: SOM (Wifi Security WPD-2 PSK) - 16.Transmission confidentiality and integrity Applicable to Smartmedic device, Tablet and Nurse Station
190	TRANSMISSION INTEGRITY (TXIG)	The system shall ensure integrity of transmitted health data	Yes	D001020115: SOM (Wifi Security WPD-2 PSK) - 16.Transmission confidentiality and integrity Applicable to Smartmedic device, Tablet and Nurse Station

Section 4. Privacy by Design filtering questions

ID	Question	Note	Answer
200	Does the device systematically process any Protected Health Information (PHI) or Personal Information (PI)?	Answer yes if the device has software with the capability to collect and process personal information; e.g. a defibrillator that collects and stores a patient name and vital signals (e.g. ECG) and is connected to a cloud system.	No
210	Is there any processing of PHI or PI as part of the product life cycle?	The product life cycle could comprise the creation of the product (e.g. planning for patient specific implants), its distribution, sale and/or maintenance.	No

Note: After this Capabilities Assessment page is completed, the remaining Controls Assessment worksheets will indicate the security and privacy controls that must be assessed.

PRODUCT SECURITY STANDARD ASSESSMENT - Security Controls Assessment	
DHF Reference:	SGTC-NPD-000-02
Product/Entity:	e bed frame and under the bed's mattress. The device can provide patient weight, turn indication and share informatio

Instructions for this worksheet

1. Refer to D0000061606 for requirements related to the PSSA. If privacy is in scope based on answers to questions in the Capabilities Assessment worksheet, the Privacy Controls Assessment worksheet must also be completed.
2. Review Section 5, noting which security controls indicate that assessment is required. Links in the sections may be used to determine the meaning of each control and control enhancement.
   Note: When the "Y" in the Assessment Required column is followed by one or more numbers, it means that the Control Enhancement(s) of the same number(s) must be assessed in connection with the Security Control.
   Note: The Logic Table worksheet demonstrates how the selected capabilities and the potential impact level determine which controls and control enhancements must be assessed.
3. In Section 5 indicate which controls will be included in the product design ("Yes" means that the control and any listed control enhancements will be incorporated). Enter justification for any assessment-required control that will not be included.
4. Clarification notes may be added to explain the method or extent to which the item will be incorporated.
5. Once a selected control is added to the software requirements, update the Traceability Reference field with traceability information (such as the number of the SRS document).

Section 5. NIST Security Controls (from NIST SP 800-53 rev4)

Controls (click control name for details)	Assessment Required? Y = Control must be assessed; Number(s) refers to control enhancement(s) that must be assessed	Include?	Justification if not using NIST control and applicable control enhancement(s)/ Clarification notes	Traceability Reference
AC-1 Access control policy and management	Y	No	Unique id provided for access to hospital, hence no access control	SOM D001020115 - Section 05. Access control policy and management
AC-2 Account management	Y	No	Unique id provided for access, no multiple roles/subjects/accounts	SOM D001020115 - Section 04. User Account Management
AC-3 Access enforcement	N	No	Unique id provided for access, no multiple roles/subjects	N/A
AC-5 Separation of duties	N	No	No seperation of duties planned in this product. All the duties are handeled by Stryker service person	N/A
AC-6 Least Privilege	N	No	Unique id provided for access, hence no privileges are accounted	N/A
AC-7 Unsuccessful logon attempts	Y	Yes		SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left.
AC-8 System use notification	Y	No	NS application runs on a system owned by HDO. Hence no control on the notifications	N/A
AC-11 Session lock	N	Yes		SRS : D001020097 - 2.1.2.5 -- The Application shall allow the user to be logged out if the session has ended or after 8 minutes of inactivity.
AC-12 Session Termination	N	No	Session gets temporarily locked/disabled, wont get terminated. No session termination enabled in this product.	N/A
AC-14 Permitted actions without identification or authentication	Y	No	Components in the product cant be accessed without authentication.	N/A
AC-17 Remote access	Y	No	No remote access enabled for any components in the product	N/A
AC-18 Wireless access	Y	Yes		SOM: D001020115 - Section 22. Cryptographic Protection & Management, handshaking mechasim to use wifi
AC-19 Access control for mobile devices	Y	Yes		SOM D001020115 - Section 05. Access control policy and management
AC-21 Information sharing	N	No	No information directly shared between the components with out provisioning	N/A
AC-23 Data mining protection	N	No	No database/storage is present in the system and hence no data mining	N/A
AC-24 Access control decisions	N	No	No authorization in scope for this system. Hence no access control decisions	N/A
AT-1 Security awareness and training policy and procedures	Y	Yes		SOM D001020115 - Section 06. Security awareness training
AT-2 Security awareness training	Y	Yes		SOM D001020115 - Section 06. Security awareness training
AT-3 Security training	Y	No	Unique id and hence no multiple roles associated with the current system.	N/A
AU-1 Audit and accountability policy and procedures	Y	No	Product is a combination of stryker & hospital components. Hence no global audit policy and procedure can be established	N/A
AU-2 Audit events	Y	Yes		SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left.
AU-3 Content of audit records	Y	Yes		SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left.
AU-4 Audit storage capacity	Y	No	Audit logging has miminal events. No constraints on the storage capacity.	N/A
AU-5 Response to audit processing failures	Y	No	Admin App is not hosted on a simple (resource constrained - H/W, Memory) device	N/A
AU-6 Audit review, analysis and reporting	Y	No	No need to review the audit log. Any malfunctioning observed can be handled through Service Manual Document	N/A
AU-7 Audit reduction and report generation	N	No	No need of audit data mining and reduction	N/A
AU-8 Time stamps	Y	Yes		SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left.
AU-9 Protection of audit information	Y	Yes		SRS D001020023 - 2.13.3 - Azure portal shall have authorized access.
AU-10 Non-repudiation	N	No	Audit generation is incorporated in the NS admin application which runs with restricted access. No chances of repudiation.	N/A
AU-11 Audit record retention	Y	No	Audit generation is incorporated in the NS admin application which runs with restricted access	N/A
AU-12 Audit generation	Y	Yes		SRS D001020097 – 2.1.2.1.1 Invalid email or password, only 3 attempts left.
AU-13 Monitoring for information disclosure	N	No	Audit generation is incorporated in the NS admin application which runs with restricted access	N/A
AU-14 Session audit	N	No		N/A
AU-15 Alternate audit capacity	N	No		N/A
AU-16 Cross-organizational auditing	N	No		N/A
CA-7 Continuous monitoring	Y	No	No security controls and information risk associated with the system. Hence continuous monitoring is not required.	N/A
CM-1 Configuration management policy and procedures	Y	No	No security controls and information systems present and any system specific configuration is not maintained	N/A
CM-2 Baseline configuration	Y	No		N/A
CM-3 Configuration change control	N	No		N/A
CM-4 Security impact analysis	Y	No		N/A
CM-5 Access restrictions for change	N	No		N/A
CM-6 Configuration settings	Y	No	None of the components in the product have configurable/customizable configuration settings (for ex: registry settings, account, file, directory permission settings, settings for functions, ports, protocols, services, and remote connections)	SOM D001020115 - Section 11. Configuration settings
CM-7 Least functionality	Y	No	No multiple functions/services associated with the product. Hence no purpose of assigning the least functionality.	N/A

Controls (click control name for details)	**Assessment Required?** Y = Control must be assessed; Number(s) refers to control enhancement(s) that must be assessed	**Include?**	**Justification if not using NIST control and applicable control enhancement(s)/ Clarification notes**	**Traceability Reference**
CM-9 Configuration management plan	**N**	No	No such maintenance/requirement of configuration plan for this product	N/A
CP-1 Contingency planning policy and procedures	**Y**	No	Product is a combination of stryker & hospital components. Hence no global audit policy and procedure can be established	N/A
CP-2 Contingency plan	**Y**	Yes		SOM D001020115 - Section 08. Contingency Plan Testing, Maintenance and Training
CP-3 Contingency training	**Y**	Yes		SOM D001020115 - Section 08. Contingency Plan Testing, Maintenance and Training
CP-4 Contingency plan testing	**Y**	Yes		SOM D001020115 - Section 08. Contingency Plan Testing, Maintenance and Training
CP-6 Alternate storage site	**N**	No	No alternate site required for storage & processing for this product	N/A
CP-7 Alternate processing site	**N**	No		N/A
CP-8 Telecommunications services	**N**	No	No telecommunications services required in this product	N/A
CP-9 Information system backup	**Y**	No	No storage is included in this product, hence no need of backup	N/A
CP-10 Information system recovery and reconstitution	**Y**	No	No recovery and reconstitution plan required in the product	N/A
CP-13 Alternative security mechanisms	**N**	No	Sufficient security is provided, no need to have additional/altervative security items beyond the standard employed methods for hospital environment.	N/A
IA-1 Identification and authentication policy and procedures	**Y**	No	Assigning to an individual a role or group is out of the scope. Unique id is provided for authentication. Identification based on individuals is not provided. No need of individual authentication & management.	SOM D001020115 -Section 04. User Account Management
IA-2 Identification and authentication (organizational users)	**Y + (1) (12)**	No		
IA-4 Identifier management	**Y**	No		
IA-5 Authenticator management	**Y + (1) (11)**	No		
IA-7 Cryptographic module authentication	**Y**	No		
IA-8 Identification and authentication (non-organizational users)	**Y + (1) (2) (3) (4)**	No		
IA-9 Service identification and authentication	**N**	No		
IA-10 Adaptive identification and authentication	**N**	No		
IA-11 Re-authentication	**N**	No		
IR-1 Incident response policy and procedures	**Y**	Yes		Incident management for the complete Smart Medic environment/platform SOM D001020115 - Section 07. Incident Management, Response, Training, Testing, Handling, Monitoring & Reporting (once it is on the market) is defined within the Corporate procedure - D0000003113 - Product Security Post Market Management.
IR-2 Incident response training	**Y**	Yes		
IR-3 Incident response testing	**N**	No	No Incident response testing required for this product	
IR-4 Incident handling	**Y**	Yes		
IR-5 Incident monitoring	**Y**	Yes		
IR-6 Incident reporting	**Y**	Yes		
IR-7 Incident response assistance	**Y**	Yes		
IR-8 Incident response plan	**Y**	Yes		
IR-9 Information spillage response	**N**	No	No classified or sensitive information in the product. Hence no case of information spillage	
IR-10 Integrated information security analysis team	**N**	No	No need to have an integrated team in this product for security analysis	
MA-1 System maintenance policy and procedures	**Y**	Yes		System maintenance for the Tablet (once it is on the market) is defined within the Corporate procedure SOM D001020115 - Section 10. System Maintenance
MA-2 Controlled maintenance	**Y**	Yes		
MA-3 Maintenance tools	**N**	No	No maintenance tools are being employed in this product.	
MA-4 Nonlocal maintenance	**Y**	Yes		
MA-5 Maintenance personnel	**Y**	Yes		
MA-6 Timely maintenance	**N**	No	It handeled as a part of Contingency plan. No need to consider here.	
MP-1 Media protection policy and procedures	**Y**	No	Product doesnt contain any digital/non-digital media. Hence no need to consider media protection. This product doesnt use any kind of media handelling/storage devices such as diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks, paper and microfilm.	N/A
MP-2 Media access	**Y**	No		N/A
MP-4 Media	**N**	No		N/A
MP-7 Media use	**Y**	No		N/A
MP-8 Media downgrading	**N**	No		N/A
PE-1 Physical and environmental protection policy and procedures	**Y**	No	The management of physical security aspects of the HDO's IT system, networks and other configuration items is a key responsibility of the HDO's IT network management.	N/A
PE-2 Physical access authorizations	**Y**	No		N/A
PE-3 Physical access control	**Y**	Yes		SOM D001020115 - Section 27. Physical locks
PE-4 Access control for transmission medium	**N**	No		N/A
PE-5 Access control for output devices	**N**	No		N/A
PE-6 Monitoring physical access	**Y**	No		N/A
PE-9 Power equipment and power cabling	**N**	No		N/A
PE-18 Location of information system components	**N**	No		N/A
PL-1 Security planning policy and procedures	**Y**	Yes	N/A	Security planning and information security program plan are shared responsibilities: (1) Stryker general: SYK has established QMS procedures and trainings for security and safety to be considered during the design&development and post market surveillance of any SW driven Medical Device from SYK. These procedures include the specification of roles & responsibilties. (2) Application specific security planning: The PSSA, the security architecture and the PS risk analysis define application specific security controls which shall be implemented in the application and considered in accompanying material (e.g service manual) (3) Customer specific provisions: The SOM establishes application specific security controls and guidance to be considered by the HDO for his security program planning purposes SOM D001020115 - 3.5 System Security Context and Intended Environment SOM D001020115 - 06. Security awareness training SOM D001020115 - 20. Security Program Integration
PL-2 System security plan	**Y**	Yes	N/A	
PL-4 Rules of behavior	**Y**	Yes	N/A	
PL-7 Security concept of operations	**N**	No	Hospitals doesn't require security concept of operations	
PL-8 Information security architecture	**N**	Yes	N/A	
PM-1 Information security program plan	**Y**	Yes	N/A	
PM-9 Risk management strategy	**Y**	Yes	N/A	
PM-12 Insider threat program	**Y**	Yes	N/A	
PM-14 Testing, training and monitoring	**Y**	Yes	N/A	
PM-15 Contacts with security groups and associations	**Y**	No	As the product is to be sold in India, there is no requirement for Security Group associations for India	N/A
PM-16 Threat awareness program	**Y**	Yes	N/A	Post market Security monitoring to be conducted as per "D0000003113 - Product Security Post Market Management". D001020020: Software Development Plan will define the periodic frequency of proactive surveillance of potential vulnerabilities

Controls (click control name for details)	Assessment Required? Y = Control must be assessed; Number(s) refers to control enhancement(s) that must be assessed	Include?	Justification if not using NIST control and applicable control enhancement(s)/ Clarification notes	Traceability Reference
PS-1 Personnel security policy and procedures	Y	Yes	N/A	The Corporate QMS product security policy and procedures define security roles and responsibilties which build the foundation for hiring, training, etc. for personal involved in product security activities
RA-5 Vulnerability scanning	Y	Yes	N/A	D001020037 - Penetration testing Protocol
SA-1 System and services acquisition policy and procedures	Y	Yes	N/A	All the details related to Software SOUP document SOUP Admin D001020054; SOUP Tablet D001020055; SOUP Nurse station application D001020056.
SA-3 System development life cycle	Y	Yes	N/A	"D0000061606 - Security and privacy in design controls" defines requirements and guidance for product development to establish product security and privacy by design (D0000061607) in medical devices and/or products that are software or contain software
SA-4 Acquisition process	Y	Yes	N/A	As Nurse Station application using 3rd party libraries, the acquisition has to be mentioned in the SRS.
SA-5 Information system documentation	Y	Yes	N/A	SOUP Admin D001020054; SOUP Tablet D001020055; SOUP Nurse station application D001020056, IFU 001-02-L-13-00-00 and Security Operations Manual (D001020115) are user documents which enable the HDO to supplement their information system documentation
SA-8 Security engineering principles	N	Yes	N/A	D0000061606 - Security and privacy in design controls D0000061607 - Privacy by design Defines security and privacy principles
SA-9 External information system services	Y	Yes	N/A	Currently, CAPTCHA is used for Second Factor Authentication.
SA-10 Developer configuration management	N	Yes	N/A	D001020020: Configuration management in Software Development plan
SA-11 Developer security testing and evaluation	N	Yes	N/A	"D0000061606 - Security and privacy in design controls" defines security testing requirements and practices
SA-12 Supply chain protection	N	No	The complete product and its purpose in hospital environment doesnt need any kind of supply chain protection.	N/A
SA-13 Trustworthiness	N	Yes	N/A	All controls which need to be considered by the HDO in order to ensure CIA are defined in the Security Operations Manual (D001020115) - Section 09. Trustworthiness- CIA Triad & Their Responsibilities
SA-14 Criticality analysis	N	No	Criticality analysis, as a part of supply chain risk management doesn't apply for this product and its usage in this hospital environment	N/A
SA-15 Development process, standards and tools	N	No	Stryker devices follow secure SDLC process. System & wireless-AP as per HDOs policies.	N/A
SA-16 Developer-provided training	N	No	All kinds of manuals provided for HDO to understand the system. No seperate training is needed from developer perspective.	N/A
SA-17 Developer security architecture and design	N	Yes		SOM D001020115 - Section 3.5 System Security Context and Intended Environment
SA-18 Tamper resistance and detection	N	No	Tablet is enclosed, no scope of tampering. System is in HDOs scope and tamper resistance & detection as per HDO policies.	N/A
SA-21 Developer screening	N	No	This product is not national/economic security interest. Hence no need for developer screening.	N/A
SC-1 System and communications protection policy and procedures	Y	Yes	N/A	Refer to HDO IT policy for commnuication with internal information system, SRS for Protection of communication channel of the system
SC-7 Boundary protection	Y	No	Hospitals are not required to create DMZ or virtual network to operate the system	N/A
SC-8 Transmission confidentiality and integrity	N	Yes	N/A	D001020115: SOM -Section 11.Transmission confidentiality and integrity
SC-12 Cryptographic key establishment and management	Y	Yes	Use of Wifi Security WPD-2 PSK and above for wifi access	SOM: D001020115 - Section 22. Cryptographic Protection & Management, handshaking mechasim to use wifi
SC-13 Cryptographic protection	Y	Yes	Use of Wifi Security WPD-2 PSK and above for wifi access	SOM: D001020115 - Section 22. Cryptographic Protection & Management, handshaking mechasim to use wifi
SC-17 Public key infrastructure certificates	N	Yes		Tablet SDD : SRS Number : 5.2.4.2 (a) IOT Provisioning
SC-25 Thin nodes	N	No	Hospital doesn't need any kind of thin nodes for this product	N/A
SC-26 Honeypots	N	No	Hospital doesn't need any kind of honeypots for this product	N/A
SC-28 Protection of information at rest	N	No	Sensitive data at rest is not present in the system to safeguard/protect.	N/A
SC-29 Heterogeneity	N	No	No group of systems required for this product to follow diversified practices.	N/A
SC-30 Concealment and misdirection	N	No	Techniques for concealment and misdirection is not required for this product in hospital environment.	N/A
SC-31 Covert channel analysis	N	No	Only single secured cloud communication channel exists (IOT provisioning) and no chance of covert channels for this product	N/A
SC-34 Non-modifiable executable programs	N	No	Modification of s/w can only be performed by service person with admin access	N/A
SC-35 Honey clients	N	No	Hospital doesn't need any kind of honeyclients for this product	N/A
SC-37 Out-of-band channels	N	No	No possibility of creating out-of-band channels as IOT device provisioning is enabled	N/A
SC-40 Wireless link protection	N	No	Wifi-AP is HDOs scope.	N/A
SC-41 Port and I/O device access	N	No	No port & I/O devices access enabled for the components in this product	N/A
SC-42 Sensor capability and data	N	No	Not possible as tablet is enclosed and access restricted	N/A
SC-43 Usage restrictions	N	No	Not possible as tablet is enclosed and access restricted	N/A
SC-44 Detonation chambers	N	No	Hospital doesn't need any kind of detonation chambers for this product	N/A
SI-1 System and information integrity policy and procedures	Y	Yes		The SOM D001020115 - Section as below

Controls (click control name for details)	**Assessment Required?** Y = Control must be assessed; Number(s) refers to control enhancement(s) that must be assessed	**Include?**	**Justification if not using NIST control and applicable control enhancement(s)/ Clarification notes**	**Traceability Reference**
SI-2 Flaw remediation	**Y**	Yes		12. System and information integrity 13. Malicious code protection 14. Information system monitoring 15. Information handling and retention 17. Security Alerts, Advisories, and Directives 18. Flaw remediation & Vulnerability Management describes any controls which may assist the HDO to keep its system integrity (e.g. backup, malware protection, etc.) Incident management for the Nurse station application (Once it is on the market) shall be handled as established with the Corporate procedure "D0000003113 - Product Security Post Market Management". SI-11 SRS ITEM: D001020097 -2.1.7.1.1 Something went wrong with API operation try again / contact API admin. D001020023-2.1.4.1.1 Something went wrong with API operation try again / contact API admin. SI-15: Complaint Handelling Procedure
SI-3 Malicious code protection	**Y**	Yes		
SI-4 Information system monitoring	**Y**	Yes		
SI-5 Security alerts, advisories, and directives	**Y**	Yes		
SI-6 Security functionality verification	**N**	No	No such features enabled in the components for this product.	
SI-7 Software and information integrity	**N**	No	NS app is a web app, hence no s/w integrity check required	
SI-8 Spam protection	**N**	No	Newly spam protection not required for this product in hospital environment. Existing HDO policies handles this.	
SI-10 Information input validation	**N**	No	No input receiving devices exists in this product	
SI-11 Error handling	**N**	Yes		
SI-12 Information handling and retention	**Y**	Yes		
SI-15 Information output filtering	**N**	No	Information processing not happening locally and getting received through web interface. Other factors (Network etc.,) are out-of-scope	
SI-17 Fail-safe procedures	**N**	Yes		

PRODUCT SECURITY STANDARD ASSESSMENT - Privacy Controls Assessment	
DHF Reference:	SGTC-NPD-000-02
Product/Entity:	bed frame and under the bed's mattress. The device can provide patient weight, turn indication and share informatio

Note: Privacy filtering questions have been answered No. PbD assessment not required.

Instructions for this worksheet

1. This page is only required if privacy is in scope, based on answers given in the Capabilities Assessment worksheet. See note above. Refer to D0000061607 for requirements related to Privacy by Design.
2. In section 6, indicate which Privacy by Design controls (and thus also their associated baseline requirements) will be incorporated into the product design. Enter justification for any item that will not be included.
3. Clarification notes may be added to explain the method or extent to which the item will be incorporated.
4. Once a selected control is added to the software requirements or project requirements, update the Traceability Reference field with traceability information (such as the number of the SRS or other document).

Section 6. Privacy Controls (fom Privacy by Design framework described in D0000061607)

Privacy by Design Families and Sub-Elements	PbD Controls (click to read full text of related baseline requirement)	Include?	Justification if not using PbD Control Baseline Requirements / Clarification notes	Traceability Reference
1. Authority & Purpose				
1.1 Authority to collect	1.1.1 Authority to collect in GDPR	No	N/A - Not Assessed because no Privacy impact.	
	1.1.2 Authority to collect in HIPAA	No	N/A - Not Assessed because no Privacy impact.	
	1.1.3 Authority to collect in architectural diagrams	No	N/A - Not Assessed because no Privacy impact.	
1.2 Purpose Specification	1.2.1 Purpose specification in architectural diagrams	No	N/A - Not Assessed because no Privacy impact.	
	1.2.2 Purpose limitation	No	N/A - Not Assessed because no Privacy impact.	
	1.2.3 Purpose definition in SOM	No	N/A - Not Assessed because no Privacy impact.	
2. Accountability, Audit, Risk Management				
2.2 Privacy Impact & Risk Assessment	2.2.1 Data Privacy Impact Assessment	No	N/A - Not Assessed because no Privacy impact.	
2.7 Privacy Enhanced System design & Development	2.7.1 Data minimization	Yes	User needs and other specs documents (like SRS) document the	application shall allow to assign and
	2.7.2 Pseudonymization	No	N/A - Not Assessed because no Privacy impact.	
	2.7.3 Anonymization	Yes	Process of patient data anonymization	application shall allow to assign and
	2.7.4 Encryption	No	N/A - Not Assessed because no Privacy impact.	
3. Data Quality & Integrity				
3.1 Data Quality	3.1.1 Data Quality Mechanism	No	N/A - Not Assessed because no Privacy impact.	
	3.1.2 Data integrity in the SOM	No	N/A - Not Assessed because no Privacy impact.	
3.2 Data Integrity & Data Integrity Board	3.2.1 Additional Data Processing Functions for Integrity	No	N/A - Not Assessed because no Privacy impact.	
4. Data Minimization & Retention				
4.1 Minimization of personally identifiable information	N/A	This sub-element is product-related, but is covered by overlapping requirements in sub-element 1.2.		
4.2 Data retention and disposal	4.2.1 Enabling deletion of data	No	N/A - Not Assessed because no Privacy impact.	
	4.2.2 Time Stamp Identification	No	N/A - Not Assessed because no Privacy impact.	
	4.2.3 Data Disposal in SOM	No	N/A - Not Assessed because no Privacy impact.	
4.3 Minimization of PII used in Testing, Training and IP	4.3.1 Use of Dummy Data for Testing	No	N/A - Not Assessed because no Privacy impact.	
5. Individual Participation & Redress				
5.1 Consent	5.1.1 Consent if Controller	No	N/A - Not Assessed because no Privacy impact.	
	5.1.2 Consent if Processor	No	N/A - Not Assessed because no Privacy impact.	
5.2 Individual Access	5.2.1 Functionality for Individual Data Access Requests	No	N/A - Not Assessed because no Privacy impact.	
5.3 Redress	5.3.1 Functionality for Individual Data Activity Requests	No	N/A - Not Assessed because no Privacy impact.	
6. Security				
6.1 Inventory of Personally Identifiable Information	N/A	This sub-element is product-related, but is covered by overlapping requirements in sub-element 1.2.		
7. Transparency				
7.1 Privacy Notice	7.1.1 Transparency if Controller	No	N/A - Not Assessed because no Privacy impact.	
8. Use Limitation				
8.1 Internal Use	8.1.1 Internal Use Policies	No	N/A - Not Assessed because no Privacy impact.	

PRODUCT SECURITY STANDARD ASSESSMENT - Logic Tables

Note: The table below defines the logic for the security portion of the Controls Assessment, but not the logic for privacy controls. For privacy, ALL items in the Controls Assessment are required to be assessed if either of the privacy-related questions on the Capabilities Assessment is answered Yes.

CAPABILITY SELECTIONS FROM THE CAPABILITITES ASSESSMENT PAGE

ALOF	AUDT	AUTH	CNFS	CSUP	DIDT	DTBK	EMRG	IGAU	MLDP	NAUT	PAUT	PLOK	RDMP	SAHD	SGUD	STCF	TXCF	TXIG
S	S			S	S	S			S	S	S	S	S	S	S	S	S	S

SELECTED POTENTIAL IMPACT LEVEL: Low

LOGIC CHART:

CAPABILITY FILTER TABLE — x = control applies for capability; S = capability SELECTED and thus control is in scope

CONTROL CODE AND DESCRIPTION	ALOF	AUDT	AUTH	CNFS	CSUP	DIDT	DTBK	EMRG	IGAU	MLDP	NAUT	PAUT	PLOK	RDMP	SAHD	SGUD	STCF	TXCF	TXIG	Potentially In Scope (impact-level agnostic)	POTENTIAL-IMPACT-BASED CONTROL DETERMINATION: NIST L	NIST M	NIST H	In Scope for Low		IMPACT-BASED CONTROL ENHANCEMENTS: LOW	MODERATE	HIGH	ACTUAL BASED ON LEVEL	COMBINED FINAL
AC-1 Access control policy and management	S		x					x					S			S				Y	Y	Y	Y	Y	AC-1				0	Y
AC-2 Account management	S		x	x				x			S	S				S				Y	Y	Y	Y	Y	AC-2		(1) (2) (3) (4)	(1) (2) (3) (4) (5) (11) (12) (13)	0	Y
AC-3 Access enforcement			x																	N	Y	Y	Y	Y	AC-3				0	N
AC-5 Separation of duties			x	x																N	N	Y	Y	N	AC-5				0	N
AC-6 Least Privilege			x	x																N	N	Y	Y	N	AC-6		(1) (2) (5) (9) (10)	(1) (2) (3) (5) (9) (10)	0	N
AC-7 Unsuccessful logon attempts	S		x								S	S								Y	Y	Y	Y	Y	AC-7				0	Y
AC-8 System use notification						S														Y	Y	Y	Y	Y	AC-8				0	Y
AC-11 Session lock	S																			Y	N	Y	Y	N	AC-11		(1)	(1)	0	N
AC-12 Session termination	S																			Y	N	Y	Y	N	AC-12				0	N
AC-14 Permitted actions without identification or authentication								x			S	S								Y	Y	Y	Y	Y	AC-14				0	Y
AC-17 Remote access			x		S						S	S								Y	Y	Y	Y	Y	AC-17		(1) (2) (3) (4)	(1) (2) (3) (4)	0	Y
AC-18 Wireless access			x								S	S								Y	Y	Y	Y	Y	AC-18		(1)	(1) (4) (5)	0	Y
AC-19 Access control for mobile devices			x								S				S					Y	Y	Y	Y	Y	AC-19		(5)	(5)	0	Y
AC-21 Information sharing		S	x			S														Y	N	Y	Y	N	AC-21				0	N
AC-23 Data mining protection	S	S	x			S														Y	N	N	N	N	AC-23				0	N
AC-24 Access control decisions	S		x																	Y	N	N	N	N	AC-24				0	N
AT-1 Security awareness and training policy and procedures						S										S				Y	Y	Y	Y	Y	AT-1				0	Y
AT-2 Security awareness training																S				Y	Y	Y	Y	Y	AT-2		(2)	(2)	0	Y
AT-3 Security training																S				Y	Y	Y	Y	Y	AT-3				0	Y
AU-1 Audit and accountability policy and procedures		S																		Y	Y	Y	Y	Y	AU-1				0	Y
AU-2 Audit events		S									S	S	S							Y	Y	Y	Y	Y	AU-2		(3)	(3)	0	Y
AU-3 Content of audit records		S				S														Y	Y	Y	Y	Y	AU-3		(1)	(1) (2)	0	Y
AU-4 Audit storage capacity		S																		Y	Y	Y	Y	Y	AU-4				0	Y
AU-5 Response to audit processing failures		S																		Y	Y	Y	Y	Y	AU-5			(1) (2)	0	Y
AU-6 Audit review, analysis and reporting		S																		Y	Y	Y	Y	Y	AU-6		(1) (3)	(1) (3) (5) (6)	0	Y
AU-7 Audit reduction and report generation		S																		Y	N	Y	Y	N	AU-7		(1)	(1)	0	N
AU-8 Time stamps		S																		Y	Y	Y	Y	Y	AU-8		(1)	(1)	0	Y
AU-9 Protection of audit information		S				S	S													Y	Y	Y	Y	Y	AU-9		(4)	(2) (3) (4)	0	Y
AU-10 Non-repudiation		S									S	S								Y	N	N	Y	N	AU-10				0	N
AU-11 Audit record retention		S				S														Y	Y	Y	Y	Y	AU-11				0	Y
AU-12 Audit generation		S																		Y	Y	Y	Y	Y	AU-12			(1) (3)	0	Y
AU-13 Monitoring for information disclosure		S																		Y	N	N	N	N	AU-13				0	N
AU-14 Session audit		S																		Y	N	N	N	N	AU-14				0	N
AU-15 Alternate audit capacity		S																		Y	N	N	N	N	AU-15				0	N
AU-16 Cross-organizational auditing		S																		Y	N	N	N	N	AU-16				0	N
CA-7 Continuous monitoring													S							Y	Y	Y	Y	Y	CA-7		(1)	(1)	0	Y
CM-1 Configuration management policy and procedures				x			S				S	S								Y	Y	Y	Y	Y	CM-1				0	Y
CM-2 Baseline configuration				x	S		S													Y	Y	Y	Y	Y	CM-2		(1) (3) (7)	(1) (2) (3) (7)	0	Y
CM-3 Configuration change control				x	S		S			S	S									Y	N	Y	Y	N	CM-3		(2)	(1) (2)	0	N
CM-4 Security impact analysis	S			x	S															Y	Y	Y	Y	Y	CM-4			(1)	0	Y
CM-5 Access restrictions for change				x	S		S													Y	N	Y	Y	N	CM-5			(1) (2) (3)	0	N
CM-6 Configuration settings				x			S				S				S					Y	Y	Y	Y	Y	CM-6		(3)	(1) (2)	0	Y
CM-7 Least functionality				x											S					Y	Y	Y	Y	Y	CM-7		(1) (2) (4)	(1) (2) (5)	0	Y
CM-9 Configuration management plan				x																N	N	Y	Y	N	CM-9				0	N
CP-1 Contingency planning policy and procedures							S									S				Y	Y	Y	Y	Y	CP-1				0	Y
CP-2 Contingency plan							S									S				Y	Y	Y	Y	Y	CP-2		(1) (3) (8)	(1) (2) (3) (4) (5) (8)	0	Y
CP-3 Contingency training							S									S				Y	Y	Y	Y	Y	CP-3			(1)	0	Y
CP-4 Contingency plan testing							S													Y	Y	Y	Y	Y	CP-4		(1)	(1) (2)	0	Y
CP-6 Alternate storage site							S						S							Y	N	Y	Y	N	CP-6		(1) (3)	(1) (2) (3)	0	N
CP-7 Alternate processing site							S													Y	N	Y	Y	N	CP-7		(1) (2) (3)	(1) (2) (3) (4)	0	N
CP-8 Telecommunications services							S													Y	N	Y	Y	N	CP-8		(1) (2)	(1) (2) (3) (4)	0	N
CP-9 Information system backup							S													Y	Y	Y	Y	Y	CP-9		(1)	(1) (2) (3) (5)	0	Y
CP-10 Information system recovery and reconstitution							S													Y	Y	Y	Y	Y	CP-10		(2)	(2) (4)	0	Y
CP-13 Alternative security mechanisms							S													Y	N	N	N	N	CP-13				0	N
IA-1 Identification and authentication policy and procedures					S			x			S	S								Y	Y	Y	Y	Y	IA-1				0	Y
IA-2 Identification and authentication (organizational users)												S								Y	Y	Y	Y	Y	IA-2	(1) (12)	(1) (2) (3) (8) (11) (12)	(1) (2) (3) (4) (8) (9) (11) (12)	(1) (12)	Y + (1) (12)
IA-4 Identifier management	S											S								Y	Y	Y	Y	Y	IA-4				0	Y
IA-5 Authenticator management												S								Y	Y	Y	Y	Y	IA-5	(1) (11)	(1) (2) (3) (11)	(1) (2) (3) (11)	(1) (11)	Y + (1) (11)
IA-7 Cryptographic module authentication												S								Y	Y	Y	Y	Y	IA-7				0	Y
IA-8 Identification and authentication (non-organizational users)												S								Y	Y	Y	Y	Y	IA-8	(1) (2) (3) (4)	(1) (2) (3) (4)	(1) (2) (3) (4)	(1) (2) (3) (4)	Y + (1) (2) (3) (4)
IA-9 Service identification and authentication					S															Y	N	N	N	N	IA-9				0	N
IA-10 Adaptive identification and authentication												S								Y	N	N	N	N	IA-10				0	N
IA-11 Re-authentication	S											S								Y	N	N	N	N	IA-11				0	N
IR-1 Incident response policy and procedures							S			S						S				Y	Y	Y	Y	Y	IR-1				0	Y
IR-2 Incident response training							S			S						S				Y	Y	Y	Y	Y	IR-2			(1) (2)	0	Y
IR-3 Incident response testing							S			S										Y	N	Y	Y	N	IR-3		(2)	(2)	0	N
IR-4 Incident handling							S			S										Y	Y	Y	Y	Y	IR-4		(1)	(1) (4)	0	Y
IR-5 Incident monitoring							S			S										Y	Y	Y	Y	Y	IR-5			(1)	0	Y
IR-6 Incident reporting							S			S										Y	Y	Y	Y	Y	IR-6		(1)	(1)	0	Y
IR-7 Incident response assistance							S			S						S				Y	Y	Y	Y	Y	IR-7		(1)	(1)	0	Y
IR-8 Incident response plan							S			S						S				Y	Y	Y	Y	Y	IR-8				0	Y
IR-9 Information spillage response							S													Y	N	N	N	N	IR-9				0	N
IR-10 Integrated information security analysis team							S													Y	N	N	N	N	IR-10				0	N
MA-1 System maintenance policy and procedures					S									S						Y	Y	Y	Y	Y	MA-1				0	Y
MA-2 Controlled maintenance					S									S						Y	Y	Y	Y	Y	MA-2			(2)	0	Y
MA-3 Maintenance tools					S					S				S						Y	N	Y	Y	N	MA-3		(1) (2)	(1) (2) (3)	0	N
MA-4 Nonlocal maintenance					S															Y	Y	Y	Y	Y	MA-4		(2)	(2) (3)	0	Y
MA-5 Maintenance personnel					S															Y	Y	Y	Y	Y	MA-5			(1)	0	Y

stryker
Form

Doc Number: D0000003422
Name: Product security standard assessment
Revision: AB

Tab: Logic Table

CAPABILITY SELECTIONS FROM THE CAPABILITITES ASSESSMENT PAGE

ALOF	AUDT	AUTH	CNFS	CSUP	DIDT	DTBK	EMRG	IGAU	MLDP	NAUT	PAUT	PLOK	RDMP	SAHD	SGUD	STCF	TXCF	TXIG
S	S			S	S	S			S	S	S	S	S	S	S	S	S	S

SELECTED POTENTIAL IMPACT LEVEL

Low

LOGIC CHART:

CAPABILITY FILTER TABLE — x = control applies for capability; S = capability SELECTED and thus control is in scope

CONTROL CODE AND DESCRIPTION	ALOF	AUDT	AUTH	CNFS	CSUP	DIDT	DTBK	EMRG	IGAU	MLDP	NAUT	PAUT	PLOK	RDMP	SAHD	SGUD	STCF	TXCF	TXIG	Potentially In Scope (impact-level agnostic)	POTENTIAL-IMPACT-BASED CONTROL DETERMINATION: NIST L	NIST M	NIST H	In Scope for Low		IMPACT-BASED CONTROL ENHANCEMENTS: LOW	MODERATE	HIGH	ACTUAL BASED ON LEVEL	COMBINED FINAL
MA-6 Timely maintenance					S									S						Y	N	Y	Y	N	MA-6				0	N
MP-1 Media protection policy and procedures					S									S						Y	Y	Y	Y	Y	MP-1				0	Y
MP-2 Media access										S			S							Y	Y	Y	Y	Y	MP-2				0	Y
MP-4 Media													S							Y	N	Y	Y	N	MP-4				0	N
MP-7 Media use													S							Y	Y	Y	Y	Y	MP-7		(1)	(1)	0	Y
MP-8 Media downgrading														S						Y	N	N	N	N	MP-8				0	N
PE-1 Physical and environmental protection policy and procedures													S							Y	Y	Y	Y	Y	PE-1				0	Y
PE-2 Physical access authorizations													S							Y	Y	Y	Y	Y	PE-2				0	Y
PE-3 Physical access control													S							Y	Y	Y	Y	Y	PE-3			(1)	0	Y
PE-4 Access control for transmission medium													S					S	S	Y	N	Y	Y	N	PE-4				0	N
PE-5 Access control for output devices													S							Y	N	Y	Y	N	PE-5				0	N
PE-6 Monitoring physical access													S							Y	Y	Y	Y	Y	PE-6		(1)	(1) (4)	0	Y
PE-9 Power equipment and power cabling													S							Y	N	Y	Y	N	PE-9				0	N
PE-18 Location of information system components													S							Y	N	N	Y	N	PE-18				0	N
PL-1 Security planning policy and procedures																S				Y	Y	Y	Y	Y	PL-1				0	Y
PL-2 System security plan													S			S				Y	Y	Y	Y	Y	PL-2		(3)	(3)	0	Y
PL-4 Rules of behavior			x													S				Y	Y	Y	Y	Y	PL-4		(1)	(1)	0	Y
PL-7 Security concept of operations																S				Y	N	N	N	N	PL-7				0	N
PL-8 Information security architecture																S				Y	N	Y	Y	N	PL-8				0	N
PM-1 Information security program plan																S				Y	Y	Y	Y	Y	PM-1				0	Y
PM-9 RISK MANAGEMENT strategy							S									S				Y	Y	Y	Y	Y	PM-9				0	Y
PM-12 Insider threat program																S				Y	Y	Y	Y	Y	PM-12				0	Y
PM-14 Testing, training and monitoring																S				Y	Y	Y	Y	Y	PM-14				0	Y
PM-15 Contacts with security groups and associations																S				Y	Y	Y	Y	Y	PM-15				0	Y
PM-16 Threat awareness program																S				Y	Y	Y	Y	Y	PM-16				0	Y
PS-1 Personnel security policy and procedures																S				Y	Y	Y	Y	Y	PS-1				0	Y
RA-5 Vulnerability scanning								x		S			S							Y	Y	Y	Y	Y	RA-5		(1) (2) (5)	(1) (2) (4) (5)	0	Y
SA-1 System and services acquisition policy and procedures														S						Y	Y	Y	Y	Y	SA-1				0	Y
SA-3 System development life cycle														S						Y	Y	Y	Y	Y	SA-3				0	Y
SA-4 Acquisition PROCESS										S				S		S				Y	Y	Y	Y	Y	SA-4		(1) (2) (9) (10)	(1) (2) (9) (10)	0	Y
SA-5 Information system documentation														S		S				Y	Y	Y	Y	Y	SA-5				0	Y
SA-8 Security engineering principles					S					S				S						Y	N	Y	Y	N	SA-8				0	N
SA-9 External information system services														S						Y	Y	Y	Y	Y	SA-9		(2)	(2)	0	Y
SA-10 Developer configuration management				x										S						Y	N	Y	Y	N	SA-10				0	N
SA-11 Developer security testing and evaluation					S									S						Y	N	Y	Y	N	SA-11				0	N
SA-12 Supply chain protection										S				S						Y	N	N	Y	N	SA-12				0	N
SA-13 Trustworthiness									x	S										Y	N	N	N	N	SA-13				0	N
SA-14 Criticality analysis					S										S					Y	N	N	N	N	SA-14				0	N
SA-15 Development PROCESS, standards and tools														S						Y	N	N	Y	N	SA-15				0	N
SA-16 Developer-provided training														S		S				Y	N	N	Y	N	SA-16				0	N
SA-17 Developer security architecture and design														S	S					Y	N	N	Y	N	SA-17				0	N
SA-18 Tamper resistance and detection															S					Y	N	N	N	N	SA-18				0	N
SA-21 Developer screening														S						Y	N	N	N	N	SA-21				0	N
SC-1 System and communications protection policy and procedures																S		S	S	Y	Y	Y	Y	Y	SC-1				0	Y
SC-7 Boundary protection										S										Y	Y	Y	Y	Y	SC-7		(3) (4) (5) (7)	(3) (4) (5) (7) (8) (18 (21)	0	Y
SC-8 Transmission confidentiality and integrity													S					S	S	Y	N	Y	Y	N	SC-8		(1)	(1)	0	N
SC-12 Cryptographic key establishment and management									x			S					S	S		Y	Y	Y	Y	Y	SC-12			(1)	0	Y
SC-13 Cryptographic protection									x								S	S		Y	Y	Y	Y	Y	SC-13				0	Y
SC-17 Public key infrastructure certificates									x								S			Y	N	Y	Y	N	SC-17				0	N
SC-25 Thin nodes															S					Y	N	N	N	N	SC-25				0	N
SC-26 Honeypots										S										Y	N	N	N	N	SC-26				0	N
SC-28 Protection of information at rest									x	S					S		S			Y	N	Y	Y	N	SC-28				0	N
SC-29 Heterogeneity															S					Y	N	N	N	N	SC-29				0	N
SC-30 Concealment and misdirection										S					S					Y	N	N	N	N	SC-30				0	N
SC-31 Covert channel analysis															S					Y	N	N	N	N	SC-31				0	N
SC-34 Non-modifiable executable programs										S										Y	N	N	N	N	SC-34				0	N
SC-35 Honey clients										S					S					Y	N	N	N	N	SC-35				0	N
SC-37 Out-of-band channels										S										Y	N	N	N	N	SC-37				0	N
SC-40 Wireless link protection															S					Y	N	N	N	N	SC-40				0	N
SC-41 Port and I/O device access															S					Y	N	N	N	N	SC-41				0	N
SC-42 Sensor capability and data															S					Y	N	N	N	N	SC-42				0	N
SC-43 Usage restrictions															S					Y	N	N	N	N	SC-43				0	N
SC-44 Detonation chambers										S										Y	N	N	N	N	SC-44				0	N
SI-1 System and information integrity policy and procedures							S		x							S			S	Y	Y	Y	Y	Y	SI-1				0	Y
SI-2 Flaw remediation										S						S				Y	Y	Y	Y	Y	SI-2		(2)	(1) (2)	0	Y
SI-3 Malicious code protection									x	S						S			S	Y	Y	Y	Y	Y	SI-3		(1) (2)	(1) (2)	0	Y
SI-4 Information system monitoring										S						S				Y	Y	Y	Y	Y	SI-4		(2) (4) (5)	(2) (4) (5)	0	Y
SI-5 Security alerts, advisories, and directives																S				Y	Y	Y	Y	Y	SI-5			(1)	0	Y
SI-6 Security functionality VERIFICATION																S				Y	N	N	Y	N	SI-6				0	N
SI-7 Software and information integrity									x	S						S				Y	N	Y	Y	N	SI-7		(1) (7)	(1) (2) (5) (7) (14)	0	N
SI-8 Spam protection																S				Y	N	Y	Y	N	SI-8		(1) (2)	(1) (2)	0	N
SI-10 Information input validation									x							S				Y	N	Y	Y	N	SI-10				0	N
SI-11 Error handling					S										S	S				Y	N	Y	Y	N	SI-11				0	N
SI-12 Information handling and retention																S				Y	Y	Y	Y	Y	SI-12				0	Y
SI-15 Information output filtering										S										Y	N	N	N	N	SI-15				0	N
SI-17 Fail-safe procedures																S				Y	N	N	N	N	SI-17				0	N

REFERENCE FOR POTENTIAL IMPACT LEVEL SELECTION

From FIPS PUB 199:

SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)},

The potential impact is LOW if—

– The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.2
AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is MODERATE if—

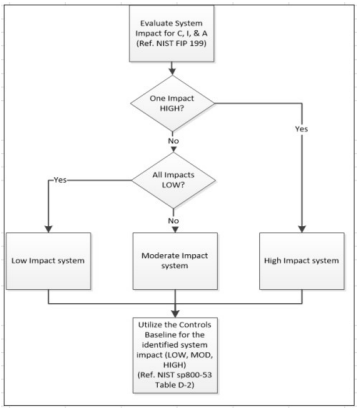
– The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is HIGH if—
– The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

A low-impact system is an information system in which all three of the security objectives are low.

A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate.
A high-impact system is an information system in which at least one security objective is high.



PRODUCT SECURITY STANDARD ASSESSMENT - Capability Explanations and MDS2 References

Capability	Explanation from AAMI/IEC TIR80001-2-8:2016	Related MDS2 Questions		NIST Security Control related to MDS2 Question
AUTOMATIC LOGOFF (ALOF)	**Requirement goal:** Reduce the RISK of unauthorized access to HEALTH DATA from an unattended workspot. Prevent misuse by other users if a system or workspot is left idle for a period of time. **User need:** Unauthorized users are not able to access HEALTH DATA at an unattended workspot. Authorized user sessions need to automatically terminate or lock after a pre-set period of time. This reduces the RISK of unauthorized access to HEALTH DATA when an authorized user left the workspot without logging off or locking the display or room. Automatic logoff needs to include a clearing of HEALTH DATA from all displays as appropriate. The local authorized IT administrator needs to be able to disable the function and set the expiration time (including screen saver) A screen saver with short inactivity time or manually enabled by a shortcut key might be an additional feature. This HEALTH DATA display clearing could be invoked when no key is pressed for some short period (e.g. 15 s to several minutes). This would not log out the user but would reduce RISK of casual viewing of information. It is desirable that clinical users should not lose uncommitted work due to automatic logoff. Consider detailing characteristics under ALOF that distinguish between (a) logoff and (b) screen locking with resumption of session.	ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	AC-12
		ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	AC-11
AUDIT CONTROLS (AUDT)	**Requirement goal:** Define harmonized approach towards reliably auditing who is doing what with HEALTH DATA, allowing HDO IT to monitor this using public frameworks, standards and technology. Our industry agreed upon and HDO IT strongly prefers Integrating the Healthcare Enterprise (IHE) audit trail profile support. Audit goal (from IHE): To allow a security officer in an institution to audit activities, to assess compliance with a secure domain's policies, to detect instances of non-compliant behaviour, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). **User need:** Capability to record and examine system activity by creating audit trails on a device to track system and HEALTH DATA access, modification, or deletion. Support for use either as a stand-alone repository (logging audit files in its own file system) or, when configured as such, will send logged information to a separate, HDO-managed central repository. Audit creation and maintenance supported by appropriate audit review tools. Securing of audit data as appropriate (especially if they contain personal data themselves). Audit data that cannot be edited or deleted. Audit data likely contains personal data and/or HEALTH DATA and all processing (e.g. access, storage and transfer) should have appropriate controls.	AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	AU-1
		AUDT-1.1	Does the audit log record a USER ID?	
		AUDT-1.2	Does other personally identifiable information exist in the audit trail?	AU-2
		AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	AU-2
		AUDT-2.1	Successful login/logout attempts?	AU-2
		AUDT-2.2	Unsuccessful login/logout attempts?	AU-2
		AUDT-2.3	Modification of user privileges?	AU-2
		AUDT-2.4	Creation/modification/deletion of users?	AU-2
		AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	AU-2
		AUDT-2.6	Creation/modification/deletion of data?	AU-2
		AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	AU-2
		AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	AU-2
		AUDT-2.8.1	Remote or on-site support?	AU-2
		AUDT-2.8.2	Application Programming Interface (API) and similar activity?	AU-2
		AUDT-2.9	Emergency access?	AU-2
		AUDT-2.10	Other events (e.g., software updates)?	AU-2
		AUDT-2.11	Is the audit capability documented in more detail?	AU-2
		AUDT-3	Can the owner/operator define or select which events are recorded in the audit log?	AU-2
		AUDT-4	Is a list of data attributes that are captured in the audit log for an event available?	AU-2
		AUDT-4.1	Does the audit log record date/time?	AU-2
		AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	AU-2
		AUDT-5	Can audit log content be exported?	AU-2
		AUDT-5.1	Via physical media?	
		AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	
		AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)?	
		AUDT-5.4	Are audit logs encrypted in transit or on storage media?	
		AUDT-6	Can audit logs be monitored/reviewed by owner/operator?	
		AUDT-7	Are audit logs protected from modification?	AU-2
		AUDT-7.1	Are audit logs protected from access?	
		AUDT-8	Can audit logs be analyzed by the device?	AU-2
AUTHORIZATION (AUTH)	**Requirement goal:** Following the principle of data minimization, provide control of access to HEALTH DATA and functions only as necessary to perform the tasks required by the HDO consistent with the INTENDED USE. **User need:** Avoiding unauthorized access to data and functions in order to (1) preserve system and data confidentiality, integrity and availability and (2) remain within permitted uses of data and systems. As defined by HDO IT policy and based on the authenticated individual user's identification, the authorization capability allows each user to only access approved data and only perform approved functions on the device. Authorized users include HDO and service staff as defined by that policy. • MEDICAL DEVICES typically support a permissions-based system providing access to system functions and data appropriate to the role(s) of the individual in the HDO (role-based access control, RBAC). For example: OPERATORS can perform their assigned tasks using all appropriate device functions (e.g. monitor or scan patients). • Quality staff (e.g. medical physicist) can engage in all appropriate quality and assurance testing activities. • Service staff can access the system in a manner that supports their preventive maintenance, problem investigation, and problem elimination activities. Authorization permits the RISK to effectively deliver healthcare while (1) maintaining system and data security and (2) following the principle of appropriate data access minimization. Authorization can be managed locally or enterprisewide (e.g. via centralized directory). Where INTENDED USE does not permit the time necessary for logging onto and off of a device (e.g. high-throughput use), the local IT Policy can permit reduced authorization controls presuming adequacy of controlled and restricted physical access.	AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	IA-2
		AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)?	IA-2
		AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)?	IA-2
		AUTH-1.3	Are any special groups, organizational units, or group policies required?	IA-2
		AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	IA-2
		AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	IA-2
		AUTH-4	Does the device authorize or control all API access requests?	IA-2
		AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default?	
CONFIGURATION OF SECURITY FEATURES (CNFS)	**Requirement goal:** To allow the HDO to determine how to utilize the product SECURITY CAPABILITIES to meet their needs for policy and/or workflow. **User need:** The local authorized IT administrator needs to be able to select the use of the product SECURITY CAPABILITIES or not to use the product SECURITY CAPABILITIES This can include aspects of privilege management interacting with SECURITY CAPABILITY control.	N/A		
CYBER SECURITY PRODUCT UPGRADES (CSUP)	**Requirement goal:** Create a unified way of working. Installation / Upgrade of product security patches by on-site service staff, remote service staff, and possibly authorized HDO staff (downloadable patches). **User need:** Installation of third party security patches on medical products as soon as possible in accordance with regulations requiring: • Highest priority is given to patches that address high-RISK vulnerabilities as judged by objective, authoritative, documented, MDM vulnerability RISK EVALUATION. • The medical product vendor and the healthcare provider are required to assure continued safe and effective clinical functionality of their products. Understanding of local MEDICAL DEVICE regulation (in general, MEDICAL DEVICES should not be patched or modified without explicit written instructions from the MDM). • Adequate testing has to be done to discover any unanticipated side effects of the patch on the medical product (performance or functionality) that might endanger a PATIENT. User, especially HDO IT staff and HDO service, requires proactive information on assessed/validated patches.	CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	
		CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	
		CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	
		CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	
		CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	
		CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	
		CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	
		CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	
		CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	
		CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	
		CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	
		CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	
		CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	
		CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	
		CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	
		CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	
		CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	
		CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	
		CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	
		CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	
		CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	
		CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or refernce in notes and complete 6.1-6.4.	
		CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	
		CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	
		CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	
		CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	
		CSUP-7	Does the manufacturer notify the customer when updates are approved for installation?	
		CSUP-8	Does the device perform automatic installation of software updates?	
		CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device?	
		CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	
		CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	
		CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	

Capability	Explanation from AAMI/IEC TIR80001-2-8:2016	Related MDS2 Questions		NIST Security Control related to MDS2 Question
		CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	
		CSUP-11.2	Is there an update review cycle for the device?	
HEALTH DATA DE-IDENTIFICATION (DIDT)	**Requirement goal:** Ability of equipment (application software or additional tooling) to directly remove information that allows identification of patient. Data scrubbing prior to shipping back to factory; architecting to allow remote service without HEALTH DATA access/exposure; in-factory quarantine, labelling, and training. **User need:** Clinical user, service engineers and marketing need to be able to de-identify HEALTH DATA for various purposes not requiring PATIENT identity.	DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information?	
		DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification?	
DATA BACKUP AND DISASTER RECOVERY (DTBK)	**Requirement goal:** Assure that the healthcare provider can continue business after damage or destruction of data, hardware, or software. **User need:** Reasonable assurance that persistent system settings and persistent HEALTH DATA stored on products can be restored after a system failure or compromise so that business can be continued. NOTE This requirement might not be appropriate for smaller, low-cost devices and can, in practice, rely on the ability to collect new, relevant data in the next acquisition cycle (e.g. short-duration heart rate data lost due to occasional wireless signal loss)	DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	
		DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	CP-9
		DTBK-3	Does the device have an integral data backup capability to removable media?	CP-9
		DTBK-4	Does the device have an integral data backup capability to remote storage?	
		DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration?	
		DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	CP-9
EMERGENCY ACCESS (EMRG)	**Requirement goal:** Ensure that access to protected HEALTH DATA is possible in case of an emergency situation requiring immediate access to stored HEALTH DATA. **User need:** During emergency situations, the clinical user needs to be able to access HEALTH DATA without personal user id and authentication (break-glass functionality). Emergency access is to be detected, recorded and reported. Ideally including some manner of immediate notification to the system administrator or medical staff (in addition to audit record). Emergency access needs to require and record self-attested user identification as entered (without authentication). HDO can solve this through procedural approach using a specific user account or function of the system. The administrator needs to be able to enable/disable any emergency functions provided by the product dependent on technical or procedural controls are required.	EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature?	SI-17
HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)	**Requirement goal:** Assure that HEALTH DATA has not been altered or destroyed in non-authorized manner and is from the originator. Assure integrity of HEALTH DATA. **User need:** User wants the assurance that HEALTH DATA is reliable and not tampered with. Solutions are to include both fixed and also removable media.	IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	SC-28
		IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	SC-28
MALWARE DETECTION/PROTECTION (MLDP)	**Requirement goal:** Product supports regulatory, HDO and user needs in ensuring an effective and uniform support for the prevention, detection and removal of malware. This is an essential step in a proper defence in depth approach to security. Malware application software is updated, malware pattern data files kept current and operating systems and applications are patched in a timely fashion. Postupdating VERIFICATION testing of device operation for both continued INTENDED USE and SAFETY is often necessary to meet regulatory quality requirements. **User need:** HDOs need to detect traditional malware as well as unauthorized software that could interfere with proper operation of the device/system.	MLDP-1	Is the device capable of hosting executable software?	
		MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	SI-3
		MLDP-2.1	Does the device include anti-malware software by default?	CM-5
		MLDP-2.2	Does the device have anti-malware software available as an option?	AU-6
		MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software?	CP-10
		MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	AU-2
		MLDP-2.5	Does notification of malware detection occur in the device user interface?	
		MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected?	
		MLDP-2.7	Are malware notifications written to a log?	
		MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	
		MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available?	SI-2
		MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device?	SI-3
		MLDP-5	Does the device employ a host-based intrusion detection/prevention system?	SI-4
		MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	CM-7
		MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	
NODE AUTHENTICATION (NAUT)	**Requirement goal:** Authentication policies need to be flexible to adapt to local HDO IT policy. As necessary, use node authentication when communicating HEALTH DATA. **User need:** Capability of managing cross-machine accounts on a modality to protect HEALTH DATA access. Support for stand-alone and central administration. Support for node authentication according to industry standards. To detect and prevent entity falsification (provide non-repudiation).	NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)?	SC-23
		NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)?	SC-7
		NAUT-2.1	Is the firewall ruleset documented and available for review?	
		NAUT-3	Does the device use certificate-based network connection authentication?	
PERSON AUTHENTICATION (PAUT)	**Requirement goal:** Authentication policies need to be flexible to adapt to HDO IT policy. This requirement as a logical place to require person authentication when providing access to HEALTH DATA. To control access to devices, network resources and HEALTH DATA and to generate non- repudiatable audit trails. This feature should be able to identify unambiguously and with certainty the individual who is accessing the network, device or resource. NOTE This requirement is relaxed during "break-glass" operation. See capability "Emergency access." **User need:** Capability of managing accounts on a modality to protect HEALTH DATA access. Desirable to link to personal settings/preferences. Support for stand-alone and central administration. Single sign-on and same password on all workspots. To detect and prevent person falsification (provide non-repudiation). Role based access control (RBAC) capability desirable.	PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	IA-2
		PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)?	IA-2
		PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)?	IA-5
		PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts?	IA-2
		PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation?	SA-4(5)
		PAUT-5	Can all passwords be changed?	
		PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules?	IA-2
		PAUT-7	Does the device support account passwords that expire periodically?	
		PAUT-8	Does the device support multi-factor authentication?	
		PAUT-9	Does the device support single sign-on (SSO)?	IA-2
		PAUT-10	Can user accounts be disabled/locked on the device?	IA-2
		PAUT-11	Does the device support biometric controls?	IA-2
		PAUT-12	Does the device support physical tokens (e.g. badge access)?	
		PAUT-13	Does the device support group authentication (e.g. hospital teams)?	
		PAUT-14	Does the application or device store or manage authentication credentials?	
		PAUT-14.1	Are credentials stored using a secure method?	
PHYSICAL LOCKS (PLOK)	**Requirement goal:** Assure that unauthorized access does not compromise the system or data confidentiality, integrity and availability. **User need:** Reasonable assurance that HEALTH DATA stored on products or media is and stays secure in a manner proportionate to the sensitivity and volume of data records on the device. Systems are reasonably free from tampering or component removal that might compromise integrity, confidentiality or availability. Tampering (including device removal) is detectable.	PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section.	PE- 3(4)
		PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	PE- 3(4)
		PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	PE- 3(4)
		PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	PE- 3(4)
ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)	**Requirement goal:** HDOs want an understanding of security throughout the full life cycle of a MEDICAL DEVICE. MDM plans such that products are sustainable throughout their life cycle according internal quality systems and external regulations. Products provided with clear statement of expected life span. Goal is to proactively manage impact of life cycle of components throughout a product's full life cycle. This commercial off-the-shelf or 3rd party software includes operating systems, database systems, report generators, medical imaging processing components etc. (assumption is that existing product creation processes already manages hardware component obsolescence). Third party includes here also internal suppliers of security vulnerable components with own life cycle and support programs. **User need:** HDO contracts, policy and regulations require that vendors maintain/support the system during product life. Updates and upgrades are expected when platform components become obsolete. HDOs and service provider show extreme care in irreversibly erasing HEALTH DATA prior to storage devices being decommissioned (discarded, reused, resold or recycled). Such activities should be logged and audited. Sales and service are well informed about security support offered per product during its life cycle.	RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development?	
		RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	
		RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates?	
		RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life?	
SYSTEM AND APPLICATION HARDENING (SAHD)	**Requirement goal:** Adjust SECURITY CONTROLS on the MEDICAL DEVICE and/or software applications such that security is maximized ("hardened") while maintaining INTENDED USE. Minimize attack vectors and overall attack surface area via port closing; service removal, etc. **User need:** User requires a system that is stable and provides just those services specified and required according to its INTENDED USE with a minimum of	SAHD-1	Is the device hardened in accordance with any industry standards?	AC-17(2)/IA-3
		SAHD-2	Has the device received any cybersecurity certifications?	SA-12(10)
		SAHD-3	Does the device employ any mechanisms for software integrity checking	
		SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	
		SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	CM-8
		SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)?	AC-3
		SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	CM-7
		SAHD-5.1	Does the device provide role-based access controls?	CM-7
		SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery?	CM-8
		SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	CM-7
		SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	CM-7
		SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled?	CM-7

Capability	Explanation from AAMI/IEC TIR80001-2-8:2016	Related MDS2 Questions		NIST Security Control related to MDS2 Question
(SAHD)	maintenance activities. HDO IT requires systems connected to their network to be secure on delivery and hardened against misuse and attacks. It is desirable for the user to inform the MDM of suspected security breaches and perceived weaknesses in user equipment.	SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled?	SA-18
		SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled?	CM-6
		SAHD-10	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled?	SI-2
		SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)?	
		SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools?	
		SAHD-13	Does the product documentation include information on operational network security scanning by users?	
		SAHD-14	Can the device be hardened beyond the default provided state?	
		SAHD-14.1	Are instructions available from vendor for increased hardening?	
		SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	
		SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device?	
SECURITY GUIDANCE (SGUD)	**Requirement goal:** Ensure that security guidance for OPERATORS and administrators of the system is available. Separate manuals for OPERATORS and administrators (including MDM sales and service) are desirable as they allow understanding of full administrative functions to be kept only by administrators. **User need:** OPERATOR should be clearly informed about his responsibilities and secure way of working with the system. The administrator needs information about managing, customizing and monitoring the system (i.e. access control lists, audit logs, etc.). Administrator needs clear understanding of SECURITY CAPABILITIES to allow HEALTH DATA RISK ASSESSMENT per appropriate regulatory requirement. Sales and service also need information about the system's SECURITY CAPABILITIES and secure way of working. It is desirable for the user to know how and when to inform the MDM of suspected security breaches and perceived weaknesses in user equipment.	SGUD-1	Does the device include security documentation for the owner/operator?	AT-2/PL-2
		SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media?	MP-6
		SGUD-3	Are all access accounts documented?	AC-6,IA-2
		SGUD-3.1	Can the owner/operator manage password control for all accounts?	
		SGUD-4	Does the product include documentation on recommended compensating controls for the device?	
HEALTH DATA STORAGE CONFIDENTIALITY (STCF)	**Requirement goal:** MDM establishes technical controls to mitigate the potential for compromise to the integrity and confidentiality of HEALTH DATA stored on products or removable media. **User need:** Reasonable assurance that HEALTH DATA stored on products or media is and stays secure. Encryption has to be considered for HEALTH DATA stored on MEDICAL DEVICES based on RISK ANALYSIS. For HEALTH DATA stored on removable media, encryption might protect confidentiality/ integrity for clinical users but also MDM service and application engineers collecting clinical data. A mechanism for encryption key management consistent with conventional use, service access, emergency "break-glass" access. Encryption method and strength takes into consideration the volume (extent of record collection/aggregation) and sensitivity of data.	STCF-1	Can the device encrypt data at rest?	SC-28
		STCF-1.1	Is all data encrypted or otherwise protected?	
		STCF-1.2	Is the data encryption capability configured by default?	
		STCF-1.3	Are instructions available to the customer to configure encryption?	
		STCF-2	Can the encryption keys be changed or configured?	SC-28
		STCF-3	Is the data stored in a database located on the device?	
		STCF-4	Is the data stored in a database external to the device?	
TRANSMISSION CONFIDENTIALITY (TXCF)	**Requirement goal:** Device meets local laws, regulations and standards (e.g. USA HIPAA, EU 95/46/EC derived national laws) according to HDO needs to ensure the confidentiality of transmitted HEALTH DATA. **User need:** Assurance that HEALTH DATA confidentiality is maintained during transmission between authenticated nodes. This allows transport of HEALTH DATA over relatively open networks and/or environment where strong HDO IT policies for HEALTH DATA integrity and confidentiality are in use. See IEC TR 80001-2-3:2012 for more information on RISK MANAGEMENT for wireless network systems.	TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	CM-7
		TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media?	CM-7
		TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	
		TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	CM-7
		TXCF-4	Are connections limited to authenticated systems?	CM-7
		TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)?	
TRANSMISSION INTEGRITY (TXIG)	**Requirement goal:** Device protects the integrity of transmitted HEALTH DATA. **User need:** Assurance that integrity of HEALTH DATA is maintained during transmission. This allows transmission of HEALTH DATA over relatively open networks or environment where strong policies for HEALTH DATA integrity are in use.	TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission?	SC-8

PRODUCT SECURITY STANDARD ASSESSMENT - Security Controls and Guidance

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
AC-1 **ACCESS CONTROL POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
AC-2 **ACCOUNT MANAGEMENT**	a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.	(1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT The organization employs automated mechanisms to support the management of information system accounts. Supplemental Guidance: The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage. (2) ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator. (3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. (4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Related controls: AU-2, AU-12. (5) ACCOUNT MANAGEMENT | INACTIVITY LOGOUT The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out]. Supplemental Guidance: Related control: SC-23. (6) ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT The information system implements the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic privilege management capabilities]. Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, dynamic access control approaches (e.g., service-oriented architectures) rely on run time access control decisions facilitated by dynamic privilege management. While user identities may remain relatively constant over time, user privileges may change more frequently based on ongoing mission/business requirements and operational needs of organizations. Dynamic privilege management can include, for example, the immediate revocation of privileges from users, as opposed to requiring that users terminate and restart their sessions to reflect any changes in privileges. Dynamic privilege management can also refer to mechanisms that change the privileges of users based on dynamic rules as opposed to editing specific user profiles. This type of privilege management includes, for example, automatic adjustments of privileges if users are operating out of their normal work times, or if information systems are under duress or in emergency maintenance situations. This control enhancement also includes the ancillary effects of privilege changes, for example, the potential changes to encryption keys used for communications. Dynamic privilege management can support requirements for information system resiliency. Related control: AC-16. (7) ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; (b) Monitors privileged role assignments; and (c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate. Supplemental Guidance: Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration. (8) ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION The information system creates [Assignment: organization-defined information system accounts] dynamically. Supplemental Guidance: Dynamic approaches for creating information system accounts (e.g., as implemented within service-oriented architectures) rely on establishing accounts (identities) at run time for entities that were previously unknown. Organizations plan for dynamic creation of information system accounts by establishing trust relationships and mechanisms with the appropriate authorities to validate related authorizations and	None
AC-3 **ACCESS ENFORCEMENT**	The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3	Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems. In addition to enforcing authorized access at the information system level and recognizing that information systems can host many applications and services in support of organizational missions and business operations, access enforcement mechanisms can also be employed at the application and service level to provide increased information security. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.	(1) ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS [Withdrawn: Incorporated into AC-6]. (2) ACCESS ENFORCEMENT | DUAL AUTHORIZATION The information system enforces dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions]. Supplemental Guidance: Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Organizations do not require dual authorization mechanisms when immediate responses are necessary to ensure public and environmental safety. Dual authorization may also be known as two-person control. Related controls: CP-9, MP-6. (3) ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL The information system enforces [Assignment: organization-defined mandatory access control policy] over all subjects and objects where the policy: (a) Is uniformly enforced across all subjects and objects within the boundary of the information system; (b) Specifies that a subject that has been granted access to information is constrained from doing any of the following; (1) Passing the information to unauthorized subjects or objects; (2) Granting its privileges to other subjects; (3) Changing one or more security attributes on subjects, objects, the information system, or information system components; (4) Choosing the security attributes and attribute values to be associated with newly created or modified objects; or (5) Changing the rules governing access control; and (c) Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges (i.e., they are trusted subjects)] such that they are not limited by some or all of the above constraints. Supplemental Guidance: Mandatory access control as defined in this control enhancement is synonymous with nondiscretionary access control, and is not constrained only to certain historical uses (e.g., implementations using the Bell-LaPadula Model). The above class of mandatory access control policies constrains what actions subjects can take with information obtained from data objects for which they have already been granted access, thus preventing the subjects from passing the information to unauthorized subjects and objects. This class of mandatory access control policies also constrains what actions subjects can take with respect to the propagation of access control privileges; that is, a subject with a privilege cannot pass that privilege to other subjects. The policy is uniformly enforced over all subjects and objects to which the information system has control. Otherwise, the access control policy can be circumvented. This enforcement typically is provided via an implementation that meets the reference monitor concept (see AC-25). The policy is bounded by the information system boundary (i.e., once the information is passed outside of the control of the system, additional means may be required to ensure that the constraints on the information remain in effect). The trusted subjects described above are granted privileges consistent with the concept of least privilege (see AC-6). Trusted subjects are only given the minimum privileges relative to the above policy necessary for satisfying organizational mission/business needs. The control is most applicable when there is some policy mandate (e.g., law, Executive Order, directive, or regulation) that establishes a policy regarding access to sensitive/classified information and some users of the information system are not authorized access to all sensitive/classified information resident in the information system. This control can operate in conjunction with AC-3 (4). A subject that is constrained in its operation by policies governed by this control is still able to operate under the less rigorous constraints of AC-3 (4), but policies governed by this control take precedence over the less rigorous constraints of AC-3 (4). For example, while a mandatory access control policy imposes a constraint preventing a subject from passing information to another subject operating at a different sensitivity label, AC-3 (4) permits the subject to pass the information to any subject with the same sensitivity label as the subject. Related controls: AC-25, SC-11. (4) ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL The information system enforces [Assignment: organization-defined discretionary access control policy] over defined subjects and objects where the policy specifies that a subject that has been granted access to information can do one or more of the following: (a) Pass the information to any other subjects or objects; (b) Grant its privileges to other subjects; (c) Change security attributes on subjects, objects, the information system, or the information system's components; (d) Choose the security attributes to be associated with newly created or revised objects; or	None
AC-5 **SEPARATION OF DUTIES**	The organization: a. Separates [Assignment: organization-defined duties of individuals]; b. Documents separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties.	A.6.1.2	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.	None	None
AC-6 **LEAST PRIVILEGE**	The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5	Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.	(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS The organization explicitly authorizes access to [Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information]. Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19. (2) LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions. Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4. (3) LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system. Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17. (4) LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS The information system provides separate processing domains to enable finer-grained allocation of user privileges. Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32. (5) LEAST PRIVILEGE | PRIVILEGED ACCOUNTS The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information mitigate risk. Related control: CM-6. (6) LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS The organization prohibits privileged access to the information system by non-organizational users. Supplemental Guidance: Related control: IA-8. (7) LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES The organization: (a) Reviews [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and (b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs. Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7. (8) LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
AC-7 **UNSUCCESSFUL LOGON ATTEMPTS**	The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.	A.9.4.2	This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.	(1) UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK [Withdrawn: Incorporated into AC-7]. (2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE The information system purges/wipes information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging/wiping requirements/techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts. Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms. Related controls: AC-19, MP-5, MP-6, SC-13.	None
AC-8 **SYSTEM USE NOTIFICATION**	The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.	A.9.4.2	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.	None	None
AC-11 **SESSION LOCK**	The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	A.11.2.8, A.11.2.9	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.	(1) SESSION LOCK | PATTERN-HIDING DISPLAYS The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image. Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.	None
AC-12 **SESSION TERMINATION**	The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].	None	This control addresses the termination of user-initiated logical sessions in contrast to SC-10 which addresses the termination of network connections that are associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, time-of-day restrictions on information system use. Related controls: SC-10, SC-23.	(1) SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS The information system: (a) Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and (b) Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions. Supplemental Guidance: Information resources to which users gain access via authentication include, for example, local workstations, databases, and password-protected websites/web-based services. Logout messages for web page access, for example, can be displayed after authenticated sessions have been terminated. However, for some types of interactive sessions including, for example, file transfer protocol (FTP) sessions, information systems typically send logout messages as final messages prior to terminating sessions.	None
AC-14 **PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**	The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.	None	This control addresses situations in which organizations determine that no identification or authentication is required in organizational information systems. Organizations may allow a limited number of user actions without identification or authentication including, for example, when individuals access public websites or other publicly accessible federal information systems, when individuals use mobile phones to receive calls, or when facsimiles are received. Organizations also identify actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypasses may occur, for example, via a software-readable physical switch that commands bypass of the logon functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not repeated, but rather to situations where identification and authentication have not yet occurred. Organizations may decide that there are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none. Related controls: CP-2, IA-2.	None	None
AC-17 **REMOTE ACCESS**	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.	(1) REMOTE ACCESS | AUTOMATED MONITORING / CONTROL The information system monitors and controls remote access methods. Supplemental Guidance: Automated monitoring and control of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of information system components (e.g., servers, workstations, notebook computers, smart phones, and tablets). Related controls: AU-2, AU-12. (2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-12, SC-13. (3) REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points. Supplemental Guidance: Limiting the number of access control points for remote accesses reduces the attack surface for organizations. Organizations consider the Trusted Internet Connections (TIC) initiative requirements for external network connections. Related control: SC-7. (4) REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS The organization: (a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and (b) Documents the rationale for such access in the security plan for the information system. Supplemental Guidance: Related control: AC-6. (5) REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS [Withdrawn: Incorporated into SI-4]. (6) REMOTE ACCESS | PROTECTION OF INFORMATION The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure. Supplemental Guidance: Related controls: AT-2, AT-3, PS-6. (7) REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS [Withdrawn: Incorporated into AC-3 (10)]. (8) REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS [Withdrawn: Incorporated into CM-7]. (9) REMOTE ACCESS | DISCONNECT / DISABLE ACCESS The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [Assignment: organization-defined time period]. Supplemental Guidance: This control enhancement requires organizations to have the capability to rapidly disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of missions/business functions and the need to eliminate immediate or future remote access to organizational information systems.	None
AC-18 **WIRELESS ACCESS**	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.	A.6.2.1, A.13.1.1, A.13.2.1	Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. Related controls: AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4.	(1) WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption. Supplemental Guidance: Related controls: SC-8, SC-13. (2) WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS [Withdrawn: Incorporated into SI-4]. (3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment. Supplemental Guidance: Related control: AC-19. (4) WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. Supplemental Guidance: Organizational authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems. Related controls: AC-3, SC-15. (5) WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries. Supplemental Guidance: Actions that may be taken by organizations to limit unauthorized use of wireless communications outside of organization-controlled boundaries include, for example: (i) reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) using directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. Prior to taking such actions, organizations can conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area. Related control: PE-19.	None
AC-19 **ACCESS CONTROL FOR MOBILE DEVICES**	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.	A.6.2.1, A.11.2.6, A.13.2.1	A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, E-readers, and tablets. Mobile devices are typically associated with a single individual and the device is usually in close proximity to the individual; however, the degree of proximity can vary depending upon on the form factor and size of the device. The merely a subset of desktop systems, depending upon the nature and intended purpose of the device. Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different classes/types of such devices. Usage restrictions and specific implementation guidance for mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Organizations are cautioned that the need to provide adequate security for mobile devices goes beyond the requirements in this control. Many safeguards and countermeasures for mobile devices are reflected in other security controls in the catalog allocated in the initial control baselines as starting points for the development of security plans and overlays using the tailoring process. There may also be some degree of overlap in the requirements articulated by the security controls within the different families of controls. AC-20 addresses mobile devices that are not organization-controlled. Related controls: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4, SC-7, SC-43, SI-3, SI-4.	(1) ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES [Withdrawn: Incorporated into MP-7]. (2) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES [Withdrawn: Incorporated into MP-7]. (3) ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER [Withdrawn: Incorporated into MP-7]. (4) ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION The organization: (a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and (b) Enforces the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information: (1) Connection of unclassified mobile devices to classified information systems is prohibited; (2) Connection of unclassified mobile devices to unclassified information systems requires approval from the authorizing official; (3) Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and (4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed. (c) Restricts the connection of classified mobile devices to classified information systems in accordance with [Assignment: organization-defined security policies]. Supplemental Guidance: Related controls: CA-6, IR-4. (5) ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices]. Supplemental Guidance: Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. Related controls: MP-5, SC-13, SC-28.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
AC-21 **INFORMATION SHARING**	The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.	None	This control applies to information that may be restricted in some manner (e.g., privileged medical information, contract-sensitive information, proprietary information, personally identifiable information, classified information related to special access programs or compartments) based on some formal or administrative determination. Depending on the particular information-sharing circumstances, sharing partners may be defined at the individual, group, or organizational level. Information may be defined by content, type, security category, or special access program/compartment. Related control: AC-3.	(1) INFORMATION SHARING | AUTOMATED DECISION SUPPORT The information system enforces information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared. (2) INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL The information system implements information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].	None
AC-23 **DATA MINING PROTECTION**	The organization employs [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to adequately detect and protect against data mining.	None	Data storage objects include, for example, databases, database records, and database fields. Data mining prevention and detection techniques include, for example: (i) limiting the types of responses provided to database queries; (ii) limiting the number/frequency of database queries to increase the work factor needed to determine the contents of such databases; and (iii) notifying organizational personnel when atypical database queries or accesses occur. This control focuses on the protection of organizational information from data mining while such information resides in organizational data stores. In contrast, AU-13 focuses on monitoring for organizational information that may have been mined or otherwise obtained from data stores and is now available as open source information residing on external sites, for example, through social networking or social media websites.	None	None
AC-24 **ACCESS CONTROL DECISIONS**	The organization establishes procedures to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.	A.9.4.1 (only partially satisfies NIST control)	Access control decisions (also known as authorization decisions) occur when authorization information is applied to specific accesses. In contrast, access enforcement occurs when information systems enforce access control decisions. While it is very common to have access control decisions and access enforcement implemented by the same entity, it is not required and it is not always an optimal implementation choice. For some architectures and distributed information systems, different entities may perform access control decisions and access enforcement.	(1) ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION The information system transmits [Assignment: organization-defined access authorization information] using [Assignment: organization-defined security safeguards] to [Assignment: organization-defined information systems] that enforce access control decisions. Supplemental Guidance: In distributed information systems, authorization processes and access control decisions may occur in separate parts of the systems. In such instances, authorization information is transmitted securely so timely access control decisions can be enforced at the appropriate locations. To support the access control decisions, it may be necessary to transmit as part of the access authorization information, supporting security attributes. This is due to the fact that in distributed information systems, there are various access control decisions that need to be made and different entities (e.g., services) make these decisions in a serial fashion, each requiring some security attributes to make the decisions. Protecting access authorization information (i.e., access control decisions) ensures that such information cannot be altered, spoofed, or otherwise compromised during transmission. (2) ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY The information system enforces access control decisions based on [Assignment: organization-defined security attributes] that do not include the identity of the user or process acting on behalf of the user. Supplemental Guidance: In certain situations, it is important that access control decisions can be made without information regarding the identity of the users issuing the requests. These are generally instances where preserving individual privacy is of paramount importance. In other situations, user identification information is simply not needed for access control decisions and, especially in the case of distributed information systems, transmitting such information with the needed degree of assurance may be very expensive or difficult to accomplish.	None
AT-1 **SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
AT-2 **SECURITY AWARENESS TRAINING**	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	A.7.2.2, A.12.2.1	Organizations determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. Related controls: AT-3, AT-4, PL-4.	(1) SECURITY AWARENESS | PRACTICAL EXERCISES The organization includes practical exercises in security awareness training that simulate actual cyber attacks. Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links. Related controls: CA-2, CA-7, CP-4, IR-3. (2) SECURITY AWARENESS | INSIDER THREAT The organization includes security awareness training on recognizing and reporting potential indicators of insider threat. Supplemental Guidance: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow employees, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, or practices. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Related controls: PL-4, PM-12, PS-3, PS-6.	None
AT-3 **ROLE-BASED SECURITY TRAINING**	The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	A.7.2.2 (only partially satisfies NIST control)	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role-based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.	(1) ROLE-BASED SECURITY TRAINING | ENVIRONMENTAL CONTROLS The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls. Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility. Organizations identify personnel with specific roles and responsibilities associated with environmental controls requiring specialized training. Related controls: PE-1, PE-13, PE-14, PE-15. (2) ROLE-BASED SECURITY TRAINING | PHYSICAL SECURITY CONTROLS The organization provides [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls. Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures). Organizations identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training. Related controls: PE-2, PE-3, PE-4, PE-5. (3) ROLE-BASED SECURITY TRAINING | PRACTICAL EXERCISES The organization includes practical exercises in security training that reinforce training objectives. Supplemental Guidance: Practical exercises may include, for example, security training for software developers that includes simulated cyber attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes. (4) ROLE-BASED SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR The organization provides training to its personnel on [Assignment: organization-defined indicators of malicious code] to recognize suspicious communications and anomalous behavior in organizational information systems. Supplemental Guidance: A well-trained workforce provides another organizational safeguard that can be employed as part of a defense-in-depth strategy to protect organizations against malicious code coming in to organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender but who appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to such suspicious email or web communications (e.g., not opening attachments, not clicking on embedded web links, and checking the source of email addresses). For this process to work effectively, all organizational personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in organizational information systems can potentially provide early warning for the presence of malicious code. Recognition of such anomalous behavior by organizational personnel can supplement automated malicious code detection and protection tools and systems employed by organizations.	None
AU-1 **AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
AU-2 **AUDIT EVENTS**	The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].	None	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.	(1) AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES [Withdrawn: Incorporated into AU-12]. (2) AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT [Withdrawn: Incorporated into AU-12]. (3) AUDIT EVENTS | REVIEWS AND UPDATES The organization reviews and updates the audited events [Assignment: organization-defined frequency]. Supplemental Guidance: Over time, the events that organizations believe should be audited may change. Reviewing and updating the set of audited events periodically is necessary to ensure that the current set is still necessary and sufficient. (4) AUDIT EVENTS | PRIVILEGED FUNCTIONS [Withdrawn: Incorporated into AC-6 (9)].	None
AU-3 **CONTENT OF AUDIT RECORDS**	The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.	A.12.4.1 (only partially satisfies NIST control)	Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.	(1) CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION The information system generates audit records containing the following additional information: [Assignment: organization-defined additional, more detailed information]. Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. (2) CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components]. Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.	None
AU-4 **AUDIT STORAGE CAPACITY**	The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].	A.12.1.3	Organizations consider the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Allocating sufficient audit storage capacity reduces the likelihood of such capacity being exceeded and resulting in the potential loss or reduction of auditing capability. Related controls: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.	(1) AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE The information system off-loads audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited. Supplemental Guidance: Off-loading is a process designed to preserve the confidentiality and integrity of audit records by moving the records from the primary information system to a secondary or alternate system. It is a common process in information systems with limited audit storage capacity; the audit storage is used only in a transitory fashion until the system can communicate with the secondary or alternate system designated for storing the audit records, at which point the information is transferred.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
AU-5 **RESPONSE TO AUDIT PROCESSING FAILURES**	The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].	None	Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Organizations may choose to define additional actions for different audit processing failures (e.g., by type, by location, by severity, or a combination of such factors). This control applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the total audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both. Related controls: AU-4, SI-12.	(1) RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity. Supplemental Guidance: Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities. (2) RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts]. Supplemental Guidance: Alerts provide organizations with urgent messages. Real-time alerts provide these messages at information technology speed (i.e., the time from event detection to alert occurs in seconds or less). (3) RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS The information system enforces configurable network communications traffic volume thresholds reflecting limits on auditing capacity and [Selection: rejects; delays] network traffic above those thresholds. Supplemental Guidance: Organizations have the capability to reject or delay the processing of network communications traffic if auditing such traffic is determined to exceed the storage capacity of the information system audit function. The rejection or delay response is triggered by the established organizational traffic volume thresholds which can be adjusted based on changes to audit storage capacity. (4) RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE The information system invokes a [Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available] in the event of [Assignment: organization-defined audit failures], unless an alternate audit capability exists. Supplemental Guidance: Organizations determine the types of audit failures that can trigger automatic information system shutdowns or degraded operations. Because of the importance of ensuring mission/business continuity, organizations may determine that the nature of the audit failure is not so severe that it warrants a complete shutdown of the information system supporting the core organizational missions/business operations. In those instances, partial information system shutdowns or operating in a degraded mode with reduced capability may be viable alternatives. Related control: AU-15.	None
AU-6 **AUDIT REVIEW, ANALYSIS, AND REPORTING**	The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles].	A.12.4.1, A.16.1.2, A.16.1.4	Audit review, analysis, and reporting covers information security-related auditing performed by organizations including, for example, auditing that results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, configuration settings, system component inventory, use of maintenance tools and nonlocal maintenance, physical access, temperature and humidity, equipment delivery and removal, communications at the information system boundaries, use of mobile code, and use of VoIP. Findings can be reported to organizational entities that include, for example, incident response team, help desk, information security group/department. If organizations are prohibited from reviewing and analyzing audit information or unable to conduct such activities (e.g., in certain national security applications or systems), the review/analysis may be carried out by other organizations granted such authority. Related controls: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3, IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC-19, SI-3, SI-4, SI-7.	(1) AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. Supplemental Guidance: Organizational processes benefiting from integrated audit review, analysis, and reporting include, for example, incident response, continuous monitoring, contingency planning, and Inspector General audits. Related controls: AU-12, PM-7. (2) AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS [Withdrawn: Incorporated into SI-4]. (3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness. Supplemental Guidance: Organization-wide situational awareness includes awareness across all three tiers of risk management (i.e., organizational, mission/business process, and information system) and supports cross-organization awareness. Related controls: AU-12, IR-4. (4) AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS The information system provides the capability to centrally review and analyze audit records from multiple components within the system. Supplemental Guidance: Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products. Related controls: AU-2, AU-12. (5) AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity. Supplemental Guidance: This control enhancement does not require vulnerability scanning, the generation of performance data, or information system monitoring. Rather, the enhancement requires that the analysis of information being otherwise produced in these areas is integrated with the analysis of audit information. Security Event and Information Management System tools can facilitate audit record aggregation/consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by organizations (with localized script adjustments, as necessary) provides more cost-effective approaches for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of vulnerability scans and correlating attack detection events with scanning results. Correlation with performance data can help uncover denial of service attacks or cyber attacks resulting in unauthorized use of resources. Correlation with system monitoring information can assist in uncovering attacks and in better relating audit information to operational situations. Related controls: AU-12, IR-4, RA-5. (6) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity. Supplemental Guidance: The correlation of physical audit information and audit logs from information systems may assist organizations in identifying examples of suspicious behavior or supporting evidence of such behavior. For example, the correlation of an individual's identity for logical access to certain information systems with the additional physical security information that the individual was actually present at the facility when the logical access occurred, may prove to be useful in investigations. (7) AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS The organization specifies the permitted actions for each [Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information. Supplemental Guidance: Organizations specify permitted actions for information system processes, roles, and/or users associated with the review, analysis, and reporting of audit records through account management techniques. Specifying permitted actions on audit information is a way to enforce the principle of least privilege. Permitted actions are enforced by the information system and include, for example, read, write, execute, append, and delete. (8) AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS The organization performs a full text analysis of audited privileged commands in a physically distinct component or subsystem of the information system, or other information system that is dedicated to that analysis. Supplemental Guidance: This control enhancement requires a distinct environment for the dedicated analysis of audit information related to privileged users without compromising such information on the information system where the users have elevated privileges including the capability to execute privileged commands. Full text analysis refers to analysis that considers the full text of privileged commands (i.e., commands and all	None
AU-7 **AUDIT REDUCTION AND REPORT GENERATION**	The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records.	None	Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit reduction and report generation capabilities do not always emanate from the same information system or from the same organizational entities conducting auditing activities. Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the information system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient. Related control: AU-6.	(1) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records]. Supplemental Guidance: Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component. Related controls: AU-2, AU-12. (2) AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH The information system provides the capability to sort and search audit records for events of interest based on the content of [Assignment: organization-defined audit fields within audit records]. Supplemental Guidance: Sorting and searching of audit records may be based upon the contents of audit record fields, for example: (i) date/time of events; (ii) user identifiers; (iii) Internet Protocol (IP) addresses involved in the event; (iv) type of event; or (v) event success/failure.	None
AU-8 **TIME STAMPS**	The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].	A.12.4.4	Time stamps generated by the information system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. Related controls: AU-3, AU-12.	(1) TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE The information system: (a) Compares the internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and (b) Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period]. Supplemental Guidance: This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network. (2) TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.	None
AU-9 **PROTECTION OF AUDIT INFORMATION**	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	A.12.4.2, A.12.4.3, A.18.1.3	Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. This control focuses on technical protection of audit information. Physical protection of audit information is addressed by media protection controls and physical and environmental protection controls. Related controls: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6.	(1) PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA The information system writes audit trails to hardware-enforced, write-once media. Supplemental Guidance: This control enhancement applies to the initial generation of audit trails (i.e., the collection of audit records that represents the audit information to be used for detection, analysis, and reporting purposes) and to the backup of those audit trails. The enhancement does not apply to the initial generation of audit records prior to being written to an audit trail. Write-once, read-many (WORM) media includes, for example, Compact Disk-Recordable (CD-R) and Digital Video Disk-Recordable (DVD-R). In contrast, the use of switchable write-protection media such as on tape cartridges or Universal Serial Bus (USB) drives results in write-protected, but not write-once, media. Related controls: AU-4, AU-5. (2) PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited. Supplemental Guidance: This control enhancement helps to ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. Related controls: AU-4, AU-5, AU-11. (3) PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools. Supplemental Guidance: Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. Related controls: AU-10, SC-12, SC-13. (4) PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users]. Supplemental Guidance: Individuals with privileged access to an information system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. This control enhancement requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges. Related control: AC-5. (5) PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION The organization enforces dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information]. Supplemental Guidance: Organizations may choose different selection options for different types of audit information. Dual authorization mechanisms require the approval of two authorized individuals in order to execute. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2. (6) PROTECTION OF AUDIT INFORMATION | READ ONLY ACCESS The organization authorizes read-only access to audit information to [Assignment: organization-defined subset of privileged users]. Supplemental Guidance: Restricting privileged user authorizations to read-only helps to limit the potential damage to organizations that could be initiated by such users (e.g., deleting audit records to cover up malicious activity).	None
AU-10 **NON-REPUDIATION**	The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].	None	Types of individual actions covered by non-repudiation include, for example, creating information, sending and receiving messages, approving information (e.g., indicating concurrence or signing a contract). Non-repudiation protects individuals against later claims by: (i) authors of not having authored particular documents; (ii) senders of not having transmitted messages; (iii) receivers of not having received messages; or (iv) signatories of not having signed documents. Non-repudiation services can be used to determine if information originated from a particular individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Organizations obtain non-repudiation services by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts). Related controls: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.	(1) NON-REPUDIATION | ASSOCIATION OF IDENTITIES The information system: (a) Binds the identity of the information producer with the information to [Assignment: organization-defined strength of binding]; and (b) Provides the means for authorized individuals to determine the identity of the producer of the information. Supplemental Guidance: This control enhancement supports audit requirements that provide organizational personnel with the means to identify who produced specific information in the event of an information transfer. Organizations determine and approve the strength of the binding between the information producer and the information based on the security category of the information and relevant risk factors. Related controls: AC-4, AC-16. (2) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY The information system: (a) Validates the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and (b) Performs [Assignment: organization-defined actions] in the event of a validation error. Supplemental Guidance: This control enhancement prevents the modification of information between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine if validations are in response to user requests or generated automatically. Related controls: AC-3, AC-4, AC-16. (3) NON-REPUDIATION | CHAIN OF CUSTODY The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released. Supplemental Guidance: Chain of custody is a process that tracks the movement of evidence through its collection, safeguarding, and analysis life cycle by documenting each person who handled the evidence, the date and time it was collected or transferred, and the purpose for the transfer. If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement ensures that only approved review functions are employed. Related controls: AC-4, AC-16. (4) NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY The information system: (a) Validates the binding of the information reviewer identity to the information at the transfer or release points prior to release/transfer between [Assignment: organization-defined security domains]; and (b) Performs [Assignment: organization-defined actions] in the event of a validation error. Supplemental Guidance: This control enhancement prevents the modification of information between review and transfer/release. The validation of bindings can be achieved, for example, by the use of cryptographic checksums. Organizations determine validations are in response to user requests or generated automatically. Related controls: AC-4, AC-16. (5) NON-REPUDIATION | DIGITAL SIGNATURES [Withdrawn: Incorporated into SI-7].	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
AU-11 **AUDIT RECORD RETENTION**	The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	A.12.4.1, A.16.1.7	Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.	(1) AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY The organization employs [Assignment: organization-defined measures] to ensure that long-term audit records generated by the information system can be retrieved. Supplemental Guidance: Measures employed by organizations to help facilitate the retrieval of audit records include, for example, converting records to newer formats, retaining equipment capable of reading the records, and retaining necessary documentation to help organizational personnel understand how to interpret the records.	None
AU-12 **AUDIT GENERATION**	The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.	A.12.4.1, A.12.4.3	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.	(1) AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL The information system compiles audit records from [Assignment: organization-defined information system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail]. Supplemental Guidance: Audit trails are time-correlated if the time stamps in the individual audit records can be reliably related to the time stamps in other audit records to achieve a time ordering of the records within organizational tolerances. Related controls: AU-8, AU-12. (2) AUDIT GENERATION | STANDARDIZED FORMATS The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format. Supplemental Guidance: Audit information that is normalized to common standards promotes interoperability and exchange of such information between dissimilar devices and information systems. This facilitates production of event information that can be more readily analyzed and correlated. Standard formats for audit records include, for example, system log records and audit records compliant with Common Event Expressions (CEE). If logging mechanisms within information systems do not conform to standardized formats, systems may convert individual audit records into standardized formats when compiling system-wide audit trails. (3) AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS The information system provides the capability for [Assignment: organization-defined individuals or roles] to change the auditing to be performed on [Assignment: organization-defined information system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds]. Supplemental Guidance: This control enhancement enables organizations to extend or limit auditing as necessary to meet organizational requirements. Auditing that is limited to conserve information system resources may be extended to address certain threat situations. In addition, auditing may be limited to a specific set of events to facilitate audit reduction, analysis, and reporting. Organizations can establish time thresholds in which audit actions are changed, for example, near real-time, within minutes, or within hours. Related control: AU-7.	None
AU-13 **MONITORING FOR INFORMATION DISCLOSURE**	The organization monitors [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.	None	Open source information includes, for example, social networking sites. Related controls: PE-3, SC-7.	(1) MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS The organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner. Supplemental Guidance: Automated mechanisms can include, for example, automated scripts to monitor new posts on selected websites, and commercial services providing notifications and alerts to organizations. (2) MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES The organization reviews the open source information sites being monitored [Assignment: organization-defined frequency].	None
AU-14 **SESSION AUDIT**	The information system provides the capability for authorized users to select a user session to capture/record or view/hear.	A.12.4.1 (only partially satisfies NIST control)	Session audits include, for example, monitoring keystrokes, tracking websites visited, and recording information and/or file transfers. Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, or standards. Related controls: AC-3, AU-4, AU-5, AU-9, AU-11.	(1) SESSION AUDIT | SYSTEM START-UP The information system initiates session audits at system start-up. (2) SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT The information system provides the capability for authorized users to capture/record and log content related to a user session. (3) SESSION AUDIT | REMOTE VIEWING / LISTENING The information system provides the capability for authorized users to remotely view/hear all content related to an established user session in real time.	None
AU-15 **ALTERNATE AUDIT CAPABILITY**	The organization provides an alternate audit capability in the event of a failure in primary audit capability that provides [Assignment: organization-defined alternate audit functionality].	None	Since an alternate audit capability may be a short-term protection employed until the failure in the primary auditing capability is corrected, organizations may determine that the alternate audit capability need only provide a subset of the primary audit functionality that is impacted by the failure. Related control: AU-5.	None	None
AU-16 **CROSS-ORGANIZATIONAL AUDITING**	The organization employs [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.	None	When organizations use information systems and/or services of external organizations, the auditing capability necessitates a coordinated approach across organizations. For example, maintaining the identity of individuals that requested particular services across organizational boundaries may often be very difficult, and doing so may prove to have significant performance ramifications. Therefore, it is often the case that cross-organizational auditing (e.g., the type of auditing capability provided by service-oriented architectures) simply captures the identity of individuals issuing requests at the initial information system, and subsequent systems record that the requests emanated from authorized individuals. Related control: AU-6.	(1) CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION The organization requires that the identity of individuals be preserved in cross-organizational audit trails. Supplemental Guidance: This control enhancement applies when there is a need to be able to trace actions that are performed across organizational boundaries to a specific individual. (2) CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION The organization provides cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements]. Supplemental Guidance: Because of the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed. For example, the audit records of one organization may not provide sufficient information to determine the appropriate or inappropriate use of organizational information resources by individuals in other organizations. In some instances, only the home organizations of individuals have the appropriate knowledge to make such determinations, thus requiring the sharing of audit information among organizations.	None
CA-7 **CONTINUOUS MONITORING**	The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].	None	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.	(1) CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis. Supplemental Guidance: Organizations can maximize the value of assessments of security controls during the continuous monitoring process by requiring that such assessments be conducted by assessors or assessment teams with appropriate levels of independence based on continuous monitoring strategies. Assessor independence provides a degree of impartiality to the monitoring process. To achieve such impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work; (iii) act as management or employees of the organizations they are serving; or (iv) place themselves in advocacy positions for the organizations acquiring their services. (2) CONTINUOUS MONITORING | TYPES OF ASSESSMENTS [Withdrawn: Incorporated into CA-2]. (3) CONTINUOUS MONITORING | TREND ANALYSES The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data. Supplemental Guidance: Trend analyses can include, for example, examining recent threat information regarding the types of threat events that have occurred within the organization or across the federal government, success rates of certain types of cyber attacks, emerging vulnerabilities in information technologies, evolving social engineering techniques, results from multiple security control assessments, the effectiveness of configuration settings, and findings from Inspectors General or auditors.	None
CM-1 **CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CM family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
CM-2 **BASELINE CONFIGURATION**	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	None	This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.	(1) BASELINE CONFIGURATION | REVIEWS AND UPDATES The organization reviews and updates the baseline configuration of the information system: (a) [Assignment: organization-defined frequency]; (b) When required due to [Assignment organization-defined circumstances]; and (c) As an integral part of information system component installations and upgrades. Supplemental Guidance: Related control: CM-5. (2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. Supplemental Guidance: Automated mechanisms that help organizations maintain consistent baseline configurations for information systems include, for example, hardware and software inventory tools, configuration management tools, and network management tools. Such tools can be deployed and/or allocated as common controls, at the information system level, or at the operating system or component level (e.g., on workstations, servers, notebook computers, network components, or mobile devices). Tools can be used, for example, to track version numbers on operating system applications, types of software installed, and current patch levels. This control enhancement can be satisfied by the implementation of CM-8 (2) for organizations that choose to combine information system component inventory and baseline configuration activities. Related controls: CM-7, RA-5. (3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback. Supplemental Guidance: Retaining previous versions of baseline configurations to support rollback may include, for example, hardware, software, firmware, configuration files, and configuration records. (4) BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE [Withdrawn: Incorporated into CM-7]. (5) BASELINE CONFIGURATION | AUTHORIZED SOFTWARE [Withdrawn: Incorporated into CM-7]. (6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS The organization maintains a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration. Supplemental Guidance: Establishing separate baseline configurations for development, testing, and operational environments helps protect information systems from unplanned/unexpected events related to development and testing activities. Separate baseline configurations allow organizations to apply the configuration management that is most appropriate for each type of configuration. For example, management of operational configurations typically emphasizes the need for stability, while management of development/test configurations requires greater flexibility. Configurations in the test environment mirror the configurations in the operational environment to the extent practicable so that the results of the testing are representative of the proposed changes to the operational systems. This control enhancement requires separate configurations but not necessarily separate physical environments. Related controls: CM-4, SC-3, SC-7. (7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return. Supplemental Guidance: When it is known that information systems, system components, or devices (e.g., notebook computers, mobile devices) will be located in high-risk areas, additional security controls may be implemented to counter the greater threat in such areas coupled with the lack of physical security relative to organizational-controlled areas. For example, organizational policies and procedures for notebook computers used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific safeguards to the device after travel is completed. Specially configured notebook computers include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified safeguards applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
CM-3 **CONFIGURATION CHANGE CONTROL**	The organization: a. Determines the types of changes to the information system that are configuration-controlled; b. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; c. Documents configuration change decisions associated with the information system; d. Implements approved configuration-controlled changes to the information system; e. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; f. Audits and reviews activities associated with configuration-controlled changes to the information system; and g. Coordinates and provides oversight for configuration change control activities through [Assignment: organization-defined configuration change control element (e.g., committee, board)] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4	Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. Typical processes for managing configuration changes to information systems include, for example, Configuration Control Boards that approve proposed changes to systems. For new development information systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards. Auditing of changes includes activities before and after changes are made to organizational information systems and the auditing activities required to implement such changes. Related controls: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.	(1) CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval; (c) Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period]; (d) Prohibit changes to the information system until designated approvals are received; (e) Document all changes to the information system; and (f) Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed. (2) CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system. Supplemental Guidance: Changes to information systems include modifications to hardware, software, or firmware components and configuration settings defined in CM-6. Organizations ensure that testing does not interfere with information system operations. Individuals/groups conducting tests understand organizational security policies and procedures, information system security policies and procedures, and the specific health, safety, and environmental risks associated with particular facilities/processes. Operational systems may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If information systems must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. If testing cannot be conducted on operational systems, organizations employ compensating controls (e.g., testing on replicated systems). (3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base. (4) CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE The organization requires an information security representative to be a member of the [Assignment: organization-defined configuration change control element]. Supplemental Guidance: Information security representatives can include, for example, senior agency information security officers, information system security officers, or information system security managers. Representation by personnel with information security expertise is important because changes to information system configurations can have unintended side effects, some of which may be security-relevant. Detecting such changes early in the process can help avoid unintended, negative consequences that could ultimately affect the security state of organizational information systems. The configuration change control element in this control enhancement reflects the change control elements defined by organizations in CM-3. (5) CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE The information system implements [Assignment: organization-defined security responses] automatically if baseline configurations are changed in an unauthorized manner. Supplemental Guidance: Security responses include, for example, halting information system processing, halting selected system functions, or issuing alerts/notifications to organizational personnel when there is an unauthorized modification of a configuration item. (6) CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT The organization ensures that cryptographic mechanisms used to provide [Assignment: organization-defined security safeguards] are under configuration management. Supplemental Guidance: Regardless of the cryptographic means employed (e.g., public key, private key, shared secrets), organizations ensure that there are processes and procedures in place to effectively manage those means. For example, if devices use certificates as a basis for identification and authentication, there needs to be a process in place to address the expiration of those certificates. Related control: SC-13.	None
CM-4 **SECURITY IMPACT ANALYSIS**	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	A.14.2.3	Organizational personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills/technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing security plans to understand security control requirements and reviewing system design documentation to understand control implementation and how specific changes might affect the controls. Security impact analyses may also include assessments of risk to better understand the impact of the changes and to determine if additional security controls are required. Security impact analyses are scaled in accordance with the security categories of the information systems. Related controls: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.	(1) SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. Supplemental Guidance: Separate test environment in this context means an environment that is physically or logically isolated and distinct from the operational environment. The separation is sufficient to ensure that activities in the test environment do not impact activities in the operational environment, and information in the operational environment is not inadvertently transmitted to the test environment. Separate environments can be achieved by physical or logical means. If physically separate test environments are not used, organizations determine the strength of mechanism required when implementing logical separation (e.g., separation achieved through virtual machines). Related controls: SA-11, SC-3, SC-7. (2) SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system. Supplemental Guidance: Implementation is this context refers to installing changed code in the operational information system. Related control: SA-11.	None
CM-5 **ACCESS RESTRICTIONS FOR CHANGE**	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1	Any changes to the hardware, software, and/or firmware components of information systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access information systems for purposes of initiating changes, including upgrades and modifications. Organizations maintain records of access to ensure that configuration change control is implemented and to support after-the-fact actions should organizations discover any unauthorized changes. Access restrictions for change also include software libraries. Access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover). Related controls: AC-3, AC-6, PE-3.	(1) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING The information system enforces access restrictions and supports auditing of the enforcement actions. Supplemental Guidance: Related controls: AU-2, AU-12, AU-6, CM-3, CM-6. (2) ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES The organization reviews information system changes [Assignment: organization-defined frequency] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred. Supplemental Guidance: Indications that warrant review of information system changes and the specific circumstances justifying such reviews may be obtained from activities carried out by organizations during the configuration change process. Related controls: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8. (3) ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization. Supplemental Guidance: Software and firmware components prevented from installation unless signed with recognized and approved certificates include, for example, software and firmware version updates, patches, service packs, device drivers, and basic input output system (BIOS) updates. Organizations can identify applicable software and firmware components by type, by specific items, or a combination of both. Digital signatures and organizational verification of such signatures, is a method of code authentication. Related controls: CM-7, SC-13, SI-7. (4) ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION The organization enforces dual authorization for implementing changes to [Assignment: organization-defined information system components and system-level information]. Supplemental Guidance: Organizations employ dual authorization to ensure that any changes to selected information system components and information cannot occur unless two qualified individuals implement such changes. The two individuals possess sufficient skills/expertise to determine if the proposed changes are correct implementations of approved changes. Dual authorization may also be known as two-person control. Related controls: AC-5, CM-3. (5) ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES The organization: (a) Limits privileges to change information system components and system-related information within a production or operational environment; and (b) Reviews and reevaluates privileges [Assignment: organization-defined frequency]. Supplemental Guidance: In many organizations, information systems support multiple core missions/business functions. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers. Related control: AC-2. (6) ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES The organization limits privileges to change software resident within software libraries. Supplemental Guidance: Software libraries include privileged programs. Related control: AC-2. (7) ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS [Withdrawn: Incorporated into SI-7].	None
CM-6 **CONFIGURATION SETTINGS**	The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	None	Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information technology products for which security-related configuration settings can be defined include, for example, mainframe computers, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific settings for information systems. The established settings become part of the systems configuration baseline. Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those information system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including, for example, information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors. Common secure configurations include the United States Government Configuration Baseline (USGCB) which affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and the defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: AC-19, CM-2, CM-3, CM-7, SI-4.	(1) CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components]. Supplemental Guidance: Related controls: CA-7, CM-4. (2) CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings]. Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring established configuration settings, or in extreme cases, halting affected information system processing. Related controls: IR-4, SI-7. (3) CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION [Withdrawn: Incorporated into SI-7]. (4) CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION [Withdrawn: Incorporated into CM-4].	None
CM-7 **LEAST FUNCTIONALITY**	The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].	A.12.5.1 (only partially satisfies NIST control)	Information systems can provide a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from single information system components, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email servers or web servers, but not both). Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related controls: AC-6, CM-2, RA-5, SA-5, SC-7.	(1) LEAST FUNCTIONALITY | PERIODIC REVIEW The organization: (a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and (b) Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure]. Supplemental Guidance: The organization can either make a determination of the relative security of the function, port, protocol, and/or service or base the security decision on the assessment of other entities. Bluetooth, FTP, and peer-to-peer networking are examples of less than secure protocols. Related controls: AC-18, CM-7, IA-2. (2) LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage]. Supplemental Guidance: Related controls: CM-8, PM-5. (3) LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE The organization ensures compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services]. Supplemental Guidance: Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functions, ports, protocols, and services. (4) LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING The organization: (a) Identifies [Assignment: organization-defined software programs not authorized to execute on the information system]; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (c) Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency]. Supplemental Guidance: The process used to identify software programs that are not authorized to execute on organizational information systems is commonly referred to as blacklisting. Organizations can implement CM-7 (5) instead of this control enhancement if whitelisting (the stronger of the two policies) is the preferred approach for restricting software program execution. Related controls: CM-6, CM-8, PM-5. (5) LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING The organization: (a) Identifies [Assignment: organization-defined software programs authorized to execute on the information system]; (b) Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and (c) Reviews and updates the list of authorized software programs [Assignment: organization-defined frequency]. Supplemental Guidance: The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting. In addition to whitelisting, organizations consider verifying the integrity of white-listed software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of white-listed software can occur either prior to execution or at system startup. Related controls: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
CM-9 **CONFIGURATION MANAGEMENT PLAN**	The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the information system and places the configuration items under configuration management; and d. Protects the configuration management plan from unauthorized disclosure and modification.	A.6.1.1 (only partially satisfies NIST control)	Configuration management plans satisfy the requirements in configuration management policies while being tailored to individual information systems. Such plans define detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. Configuration management plans are typically developed during the development/acquisition phase of the system development life cycle. The plans describe how to move changes through change management processes, how to update configuration settings and baselines, how to maintain information system component inventories, how to control development, test, and operational environments, and how to develop, release, and update key documents. Organizations can employ templates to help ensure consistent and timely development and implementation of configuration management plans. Such templates can represent a master configuration management plan for the organization at large with subsets of the plan implemented on a system by system basis. Configuration management approval processes include designation of key management stakeholders responsible for reviewing and approving proposed changes to information systems, and personnel that conduct security impact analyses prior to the implementation of changes to the systems. Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration-managed. As information systems continue through the system development life cycle, new configuration items may be identified and some existing configuration items may no longer need to be under configuration control. Related controls: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.	(1) CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in information system development. Supplemental Guidance: In the absence of dedicated configuration management teams assigned within organizations, system developers may be tasked to develop configuration management processes using personnel who are not directly involved in system development or integration. This separation of duties ensures that organizations establish and maintain a sufficient degree of independence between the information system development and integration processes and configuration management processes to facilitate quality control and more effective oversight.	None
CP-1 **CONTINGENCY PLANNING POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency planning procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the CP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
CP-2 **CONTINGENCY PLAN**	The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification.	A.6.1.1, A.17.1.1, A.17.2.1	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.	(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan development with organizational elements responsible for related plans. Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, Insider Threat Implementation Plan, and Occupant Emergency Plans. (2) CONTINGENCY PLAN | CAPACITY PLANNING The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. Supplemental Guidance: Capacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning. (3) CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of essential missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12. (4) CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS The organization plans for the resumption of all missions and business functions within [Assignment: organization-defined time period] of contingency plan activation. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. The time period for resumption of all missions/business functions may be dependent on the severity/extent of disruptions to the information system and its supporting infrastructure. Related control: PE-12. (5) CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12. (6) CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE The organization plans for the transfer of essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through information system restoration to primary processing and/or storage sites. Supplemental Guidance: Organizations may choose to carry out the contingency planning activities in this control enhancement as part of organizational business continuity planning including, for example, as part of business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency (e.g., backup sites may become primary sites). Related control: PE-12. (7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS The organization coordinates its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied. Supplemental Guidance: When the capability of an organization to successfully carry out its core missions/business functions is dependent on external service providers, developing a timely and comprehensive contingency plan may become more challenging. In this situation, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization. Related control: SA-9. (8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS	None
CP-3 **CONTINGENCY TRAINING**	The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	A.7.2.2 (only partially satisfies NIST control)	Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to set up information systems at alternate processing and storage sites; and managers/senior leaders may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles/responsibilities reflects the specific continuity requirements in the contingency plan. Related controls: AT-2, AT-3, CP-2, IR-2.	(1) CONTINGENCY TRAINING | SIMULATED EVENTS The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations. (2) CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS The organization employs automated mechanisms to provide a more thorough and realistic contingency training environment.	None
CP-4 **CONTINGENCY PLAN TESTING**	The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.	A.17.1.3	Methods for testing contingency plans to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises. Organizations conduct testing based on the continuity requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals arising due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions. Related controls: CP-2, CP-3, IR-3.	(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan testing with organizational elements responsible for related plans. Supplemental Guidance: Plans related to contingency plans for organizational information systems include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. This control enhancement does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. It does require, however, that if such organizational elements are responsible for related plans, organizations should coordinate with those elements. Related controls: IR-8, PM-8. (2) CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE The organization tests the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations. Supplemental Guidance: Related control: CP-7. (3) CONTINGENCY PLAN TESTING | AUTOMATED TESTING The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan. Supplemental Guidance: Automated mechanisms provide more thorough and effective testing of contingency plans, for example: (i) by providing more complete coverage of contingency issues; (ii) by selecting more realistic test scenarios and environments; and (iii) by effectively stressing the information system and supported missions. (4) CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing. Supplemental Guidance: Related controls: CP-10, SC-24.	None
CP-6 **ALTERNATE STORAGE SITE**	The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.	A.11.1.4, A.17.1.2, A.17.2.1	Alternate storage sites are sites that are geographically distinct from primary storage sites. An alternate storage site maintains duplicate copies of information and data in the event that the primary storage site is not available. Items covered by alternate storage site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-7, CP-9, CP-10, MP-4.	(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats. Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3. (2) ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. (3) ALTERNATE STORAGE SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include, for example: (i) duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites; or (ii) planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted. Related control: RA-3.	None
CP-7 **ALTERNATE PROCESSING SITE**	The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site.	A.11.1.4, A.17.1.2, A.17.2.1	Alternate processing sites are sites that are geographically distinct from primary processing sites. An alternate processing site provides processing capability in the event that the primary processing site is not available. Items covered by alternate processing site agreements include, for example, environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and coordination for the transfer/assignment of personnel. Requirements are specifically allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. Related controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.	(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats. Supplemental Guidance: Threats that affect alternate processing sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3. (2) ALTERNATE PROCESSING SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. Supplemental Guidance: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope (e.g., hurricane, regional power outage) with such determinations made by organizations based on organizational assessments of risk. Related control: RA-3. (3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). Supplemental Guidance: Priority-of-service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources at the alternate processing site. (4) ALTERNATE PROCESSING SITE | PREPARATION FOR USE The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions. Supplemental Guidance: Site preparation includes, for example, establishing configuration settings for information system components at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and other logistical considerations are in place. Related controls: CM-2, CM-6. (5) ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS [Withdrawn: Incorporated into CP-7]. (6) ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE The organization plans and prepares for circumstances that preclude returning to the primary processing site.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
CP-8 **TELECOMMUNICATIONS SERVICES**	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.	A.11.2.2, A.17.1.2	This control applies to telecommunications services (data and voice) for primary and alternate processing and storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary/alternate sites. Alternate telecommunications services include, for example, additional organizational or commercial ground-based circuits/lines or satellites in lieu of ground-based communications. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements. Related controls: CP-2, CP-6, CP-7.	(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and (b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. Supplemental Guidance: Organizations consider the potential mission/business impact in situations where telecommunications service providers are servicing other organizations with similar priority-of-service provisions. (2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services. (3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats. Supplemental Guidance: Threats that affect telecommunications services are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber/physical attacks, and errors of omission/commission. Organizations seek to reduce common susceptibilities by, for example, minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services meeting the separation needs addressed in the risk assessment. (4) TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN The organization: (a) Requires primary and alternate telecommunications service providers to have contingency plans; (b) Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and (c) Obtains evidence of contingency testing/training by providers [Assignment: organization-defined frequency]. Supplemental Guidance: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security, state, and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training. (5) TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING The organization tests alternate telecommunication services [Assignment: organization-defined frequency].	None
CP-9 **INFORMATION SYSTEM BACKUP**	The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.	A.12.3.1, A.17.1.2, A.18.1.3	System-level information includes, for example, system-state information, operating system and application software, and licenses. User-level information includes any information other than system-level information. Mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes. Protection of system backup information while in transit is beyond the scope of this control. Information system backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Related controls: CP-2, CP-6, MP-4, MP-5, SC-13.	(1) INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity. Supplemental Guidance: Related control: CP-4. (2) INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. Supplemental Guidance: Related control: CP-4. (3) INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system. Supplemental Guidance: Critical information system software includes, for example, operating systems, cryptographic key management systems, and intrusion detection/prevention systems. Security-related information includes, for example, organizational inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities for organizations. Related controls: CM-2, CM-8. (4) INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION [Withdrawn: Incorporated into CP-9]. (5) INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE The organization transfers information system backup information to the alternate storage site [Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives]. Supplemental Guidance: Information system backup information can be transferred to alternate storage sites either electronically or by physical shipment of storage media. (6) INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM The organization accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations. Supplemental Guidance: Related controls: CP-7, CP-10. (7) INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION The organization enforces dual authorization for the deletion or destruction of [Assignment: organization-defined backup information]. Supplemental Guidance: Dual authorization ensures that the deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting/destroying backup information possess sufficient skills/expertise to determine if the proposed deletion/destruction of backup information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. Related controls: AC-3, MP-2.	None
CP-10 **INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	A.17.1.2	Recovery is executing information system contingency plan activities to restore organizational missions/business functions. Reconstitution takes place following recovery and includes activities for returning organizational information systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities, recovery point/time and reconstitution objectives, and established organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of any interim information system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored information system capabilities, reestablishment of continuous monitoring activities, potential information system reauthorizations, and activities to prepare the systems against future disruptions, compromises, or failures. Recovery/reconstitution capabilities employed by organizations can include both automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.	(1) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING [Withdrawn: Incorporated into CP-4]. (2) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY The information system implements transaction recovery for systems that are transaction-based. Supplemental Guidance: Transaction-based information systems include, for example, database management systems and transaction processing systems. Mechanisms supporting transaction recovery include, for example, transaction rollback and transaction journaling. (3) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS [Withdrawn: Addressed through tailoring procedures]. (4) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD The organization provides the capability to restore information system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components. Supplemental Guidance: Restoration of information system components includes, for example, reimaging which restores components to known, operational states. Related control: CM-2. (5) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY [Withdrawn: Incorporated into SI-13]. (6) INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION The organization protects backup and restoration hardware, firmware, and software. Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software components includes both physical and technical safeguards. Backup and restoration software includes, for example, router tables, compilers, and other security-relevant system software. Related controls: AC-3, AC-6, PE-3. References: Federal Continuity Directive 1;	None
CP-13 **ALTERNATIVE SECURITY MECHANISMS**	The organization employs [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.	A.17.1.2 (only partially satisfies NIST control)	This control supports information system resiliency and contingency planning/continuity of operations. To ensure mission/business continuity, organizations can implement alternative or supplemental security mechanisms. These mechanisms may be less effective than the primary mechanisms (e.g., not as easy to use, not as scalable, or not as secure). However, having the capability to readily employ these alternative/supplemental mechanisms enhances overall mission/business continuity that might otherwise be adversely impacted if organizational operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, this control would typically be applied only to critical security capabilities provided by information systems, system components, or information system services. For example, an organization may issue to senior executives and system administrators one-time pads in case multifactor tokens, the organization's standard means for secure remote authentication, is compromised. Related control: CP-2.	None	None
IA-1 **IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
IA-2 **IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	A.9.2.1	Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.	(1) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for network access to privileged accounts. Supplemental Guidance: Related control: AC-6. (2) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS The information system implements multifactor authentication for network access to non-privileged accounts. (3) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for local access to privileged accounts. Supplemental Guidance: Related control: AC-6. (4) IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS The information system implements multifactor authentication for local access to non-privileged accounts. (5) IDENTIFICATION AND AUTHENTICATION | GROUP AUTHENTICATION The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed. Supplemental Guidance: Requiring individuals to use individual authenticators as a second level of authentication helps organizations to mitigate the risk of using group authenticators. (6) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. Supplemental Guidance: Related control: AC-6. (7) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE The information system implements multifactor authentication for network access to non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. (8) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT The information system implements replay-resistant authentication mechanisms for network access to privileged accounts. Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators. (9) IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts. Supplemental Guidance: Authentication processes resist replay attacks if it is impractical to achieve successful authentications by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use nonces or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators. (10) IDENTIFICATION AND AUTHENTICATION | SINGLE SIGN-ON The information system provides a single sign-on capability for [Assignment: organization-defined information system accounts and services]. Supplemental Guidance: Single sign-on enables users to log in once and gain access to multiple information system resources. Organizations consider the operational efficiencies provided by single sign-on capabilities with the increased risk from disclosures of single authenticators providing access to multiple system resources. (11) IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements]. Supplemental Guidance: For remote access to privileged/non-privileged accounts, the purpose of requiring a device that is separate from the information system gaining access for one of the factors during multifactor	None
IA-4 **IDENTIFIER MANAGEMENT**	The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].	A.9.2.1	Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). Typically, individual identifiers are the user names of the information system accounts assigned to those individuals. In such instances, the account management activities of AC-2 use account names provided by IA-4. This control also addresses individual identifiers not necessarily associated with information system accounts (e.g., identifiers used in physical security control databases accessed by badge reader systems for access to information systems). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices. Related controls: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.	(1) IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts. Supplemental Guidance: Prohibiting the use of information systems account identifiers that are the same as some public identifier such as the individual identifier section of an electronic mail address, makes it more difficult for adversaries to guess user identifiers on organizational information systems. Related control: AT-2. (2) IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION The organization requires that the registration process to receive an individual identifier includes supervisor authorization. (3) IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION The organization requires multiple forms of certification of individual identification be presented to the registration authority. Supplemental Guidance: Requiring multiple forms of identification, such as documentary evidence or a combination of documents and biometrics, reduces the likelihood of individuals using fraudulent identification to establish an identity, or at least increases the work factor of potential adversaries. (4) IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS The organization manages individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status]. Supplemental Guidance: Characteristics identifying the status of individuals include, for example, contractors and foreign nationals. Identifying the status of individuals by specific characteristics provides additional information about the people with whom organizational personnel are communicating. For example, it might be useful for a government employee to know that one of the individuals on an email message is a contractor. Related control: AT-2. (5) IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT The information system dynamically manages identifiers. Supplemental Guidance: In contrast to conventional approaches to identification which presume static accounts for preregistered users, many distributed information systems including, for example, service-oriented architectures, rely on establishing identifiers at run time for entities that were previously unknown. In these situations, organizations anticipate and provision for the dynamic establishment of identifiers. Preestablished trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential. Related control: AC-16. (6) IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT The organization coordinates with [Assignment: organization-defined external organizations] for cross-organization management of identifiers. Supplemental Guidance: Cross-organization identifier management provides the capability for organizations to appropriately identify individuals, groups, roles, or devices when conducting cross-organization activities involving the processing, storage, or transmission of information. (7) IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION The organization requires that the registration process to receive an individual identifier be conducted in person before a designated registration authority. Supplemental Guidance: In-person registration reduces the likelihood of fraudulent identifiers being issued because it requires the physical presence of individuals and actual face-to-face interactions with designated registration authorities.	None
IA-5 **AUTHENTICATOR MANAGEMENT**	The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3	Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.	(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; (c) Stores and transmits only cryptographically-protected passwords; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; (e) Prohibits password reuse for [Assignment: organization-defined number] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password. Supplemental Guidance: This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6. (2) AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network. Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or certificate status protocol responses. For PIV cards, validation of certifications involves the construction and verification of a certification path to the Common Policy Root trust anchor including certificate policy processing. Related control: IA-6. (3) AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles]. (4) AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [Assignment: organization-defined requirements]. Supplemental Guidance: This control enhancement focuses on the creation of strong passwords and the characteristics of such passwords (e.g., complexity) prior to use, the enforcement of which is carried out by organizational information systems in IA-5 (1). Related controls: CA-2, CA-7, RA-5. (5) AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY The organization requires developers/installers of information system components to provide unique authenticators or change default authenticators prior to delivery/installation. Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation. However, it typically does not apply to the developers of commercial off-the-shelve information technology products. Requirements for unique authenticators can be included in acquisition documents prepared by organizations when procuring information systems or system components. (6) AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.	None
IA-7 **CRYPTOGRAPHIC MODULE AUTHENTICATION**	The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	A.18.1.5	Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Related controls: SC-12, SC-13.	None	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
IA-8 **IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	A.9.2.1	Non-organizational users include information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Organizations use risk assessments to determine authentication needs and consider scalability, practicality, and security in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk. IA-2 addresses identification and authentication requirements for access to information systems by organizational users. Related controls: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.	(1) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. Supplemental Guidance: This control enhancement applies to logical access control systems (LACS) and physical access control systems (PACS). Personal Identity Verification (PIV) credentials are those credentials issued by federal agencies that conform to FIPS Publication 201 and supporting guidance documents. OMB Memorandum 11-11 requires federal agencies to continue implementing the requirements specified in HSPD-12 to enable agency-wide use of PIV credentials. Related controls: AU-2, PE-3, SA-4. (2) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS The information system accepts only FICAM-approved third-party credentials. Supplemental Guidance: This control enhancement typically applies to organizational information systems that are accessible to the general public, for example, public-facing websites. Third-party credentials are those credentials issued by nonfederal government entities approved by the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative. Approved third-party credentials meet or exceed the set of minimum federal government-wide technical, security, privacy, and organizational maturity requirements. This allows federal government relying parties to trust such credentials at their approved assurance levels. Related control: AU-2. (3) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials. Supplemental Guidance: This control enhancement typically applies to information systems that are accessible to the general public, for example, public-facing websites. FICAM-approved information system components include, for example, information technology products and software libraries that have been approved by the Federal Identity, Credential, and Access Management conformance program. Related control: SA-4. (4) IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES The information system conforms to FICAM-issued profiles. Supplemental Guidance: This control enhancement addresses open identity management standards. To ensure that these standards are viable, robust, reliable, sustainable (e.g., available in commercial information technology products), and interoperable as documented, the United States Government assesses and scopes identity management standards and technology implementations against applicable federal legislation, directives, policies, and requirements. The result is FICAM-issued implementation profiles of approved protocols (e.g., FICAM authentication protocols such as SAML 2.0 and OpenID 2.0, as well as other protocols such as the FICAM Backend Attribute Exchange). Related control: SA-4. (5) IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV-I CREDENTIALS The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials. Supplemental Guidance: This control enhancement: (i) applies to logical and physical access control systems; and (ii) addresses Non-Federal Issuers (NFIs) of identity cards that desire to interoperate with United States Government Personal Identity Verification (PIV) information systems and that can be trusted by federal government-relying parties. The X.509 certificate policy for the Federal Bridge Certification Authority (FBCA) addresses PIV-I requirements. The PIV-I card is suitable for Assurance Level 4 as defined in OMB Memorandum 04-04 and NIST Special Publication 800-63, and multifactor authentication as defined in NIST Special Publication 800-116. PIV-I credentials are those credentials issued by a PIV-I provider whose PIV-I certificate policy maps to the Federal Bridge PIV-I Certificate Policy. A PIV-I provider is cross-certified (directly or through another PKI bridge) with the FBCA with policies that have been mapped and approved as meeting the requirements of the PIV-I policies defined in the FBCA certificate policy. Related control: AU-2.	None
IA-9 **SERVICE IDENTIFICATION AND AUTHENTICATION**	The organization identifies and authenticates [Assignment: organization-defined information system services] using [Assignment: organization-defined security safeguards].	None	This control supports service-oriented architectures and other distributed architectural approaches requiring the identification and authentication of information system services. In such architectures, external services often appear dynamically. Therefore, information systems should be able to determine in a dynamic manner, if external providers and associated services are authentic. Safeguards implemented by organizational information systems to validate provider and service authenticity include, for example, information or code signing, provenance graphs, and/or electronic signatures indicating or including the sources of services.	(1) SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE The organization ensures that service providers receive, validate, and transmit identification and authentication information. (2) SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS The organization ensures that identification and authentication decisions are transmitted between [Assignment: organization-defined services] consistent with organizational policies. Supplemental Guidance: For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of identification and authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide the identification and authentication decisions (as opposed to the actual identifiers and authenticators) to the services that need to act on those decisions. Related control: SC-8.	None
IA-10 **ADAPTIVE IDENTIFICATION AND AUTHENTICATION**	The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].	None	Adversaries may compromise individual authentication mechanisms and subsequently attempt to impersonate legitimate users. This situation can potentially occur with any authentication mechanisms employed by organizations. To address this threat, organizations may employ specific techniques/mechanisms and establish protocols to assess suspicious behavior (e.g., individuals accessing information that they do not typically access as part of their normal duties, roles, or responsibilities, accessing greater quantities of information than the individuals would routinely access, or attempting to access information from suspicious network addresses). In these situations when certain preestablished conditions or triggers occur, organizations can require selected individuals to provide additional authentication information. Another potential use for adaptive identification and authentication is to increase the strength of mechanism based on the number and/or types of records being accessed. Related controls: AU-6, SI-4.	None	None
IA-11 **RE-AUTHENTICATION**	The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].	None	In addition to the re-authentication requirements associated with session locks, organizations may require re-authentication of individuals and/or devices in other situations including, for example: (i) when authenticators change; (ii), when roles change; (iii) when security categories of information systems change; (iv), when the execution of privileged functions occurs; (v) after a fixed period of time; or (vi) periodically. Related control: AC-11.	None	None
IR-1 **INCIDENT RESPONSE POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
IR-2 **INCIDENT RESPONSE TRAINING**	The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.	A.7.2.2 (only partially satisfies NIST control)	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.	(1) INCIDENT RESPONSE TRAINING | SIMULATED EVENTS The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
IR-3 **INCIDENT RESPONSE TESTING**	The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results.	None	Organizations test incident response capabilities to determine the overall effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel/full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response. Related controls: CP-4, IR-8.	(1) INCIDENT RESPONSE TESTING | AUTOMATED TESTING The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability. Supplemental Guidance: Organizations use automated mechanisms to more thoroughly and effectively test incident response capabilities, for example: (i) by providing more complete coverage of incident response issues; (ii) by selecting more realistic test scenarios and test environments; and (iii) by stressing the response capability. Related control: AT-2. (2) INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS The organization coordinates incident response testing with organizational elements responsible for related plans. Supplemental Guidance: Organizational plans related to incident response testing include, for example, Business Continuity Plans, Contingency Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.	None
IR-4 **INCIDENT HANDLING**	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.	A.16.1.4, A.16.1.5, A.16.1.6	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process. Supplemental Guidance: Automated mechanisms supporting incident handling processes include, for example, online incident management systems. (2) INCIDENT HANDLING | DYNAMIC RECONFIGURATION The organization includes dynamic reconfiguration of [Assignment: organization-defined information system components] as part of the incident response capability. Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways. Organizations perform dynamic reconfiguration of information systems, for example, to stop attacks, to misdirect attackers, and to isolate components of systems, thus limiting the extent of the damage from breaches or compromises. Organizations include time frames for achieving the reconfiguration of information systems in the definition of the reconfiguration capability, considering the potential need for rapid response in order to effectively address sophisticated cyber threats. Related controls: AC-2, AC-4, AC-16, CM-2, CM-3, CM-4. (3) INCIDENT HANDLING | CONTINUITY OF OPERATIONS The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incidents] to ensure continuation of organizational missions and business functions. Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Appropriate incident response actions include, for example, graceful degradation, information system shutdown, fall back to manual mode/alternative technology whereby the system operates differently, employing deceptive measures, alternate information flows, or operating in a mode that is reserved solely for when systems are under attack. (4) INCIDENT HANDLING | INFORMATION CORRELATION The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. Supplemental Guidance: Sometimes the nature of a threat event, for example, a hostile cyber attack, is such that it can only be observed by bringing together information from different sources including various reports and reporting procedures established by organizations. (5) INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM The organization implements a configurable capability to automatically disable the information system if [Assignment: organization-defined security violations] are detected. (6) INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES The organization implements incident handling capability for insider threats. Supplemental Guidance: While many organizations address insider threat incidents as an inherent part of their organizational incident response capability, this control enhancement provides additional emphasis on this type of threat and the need for specific incident handling capabilities (as defined within organizations) to provide appropriate and timely responses. (7) INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION The organization coordinates incident handling capability for insider threats across [Assignment: organization-defined components or elements of the organization]. Supplemental Guidance: Incident handling for insider threat incidents (including preparation, detection and analysis, containment, eradication, and recovery) requires close coordination among a variety of organizational components or elements to be effective. These components or elements include, for example, mission/business owners, information system owners, human resources offices, procurement offices, personnel/physical security offices, operations personnel, and risk executive (function). In addition, organizations may require external support from federal, state, and local law enforcement agencies. (8) INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses. Supplemental Guidance: The coordination of incident information with external organizations including, for example, mission/business partners, military/coalition partners, customers, and multitiered developers, can provide significant benefits. Cross-organizational coordination with respect to incident handling can serve as an important risk management capability. This capability allows organizations to leverage critical information from a variety of sources to effectively respond to information security-related incidents potentially affecting the organization's operations, assets, and individuals.	None
IR-5 **INCIDENTMONITORING**	The organization tracks and documents information system security incidents.	None	Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	(1) INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-7, IR-4.	None
IR-6 **INCIDENT REPORTING**	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities].	A.6.1.3, A.16.1.2	The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. Suspected security incidents include, for example, the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5, IR-8.	(1) INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents. Supplemental Guidance: Related control: IR-7. (2) INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS The organization reports information system vulnerabilities associated with reported security incidents to [Assignment: organization-defined personnel or roles]. (3) INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN The organization provides security incident information to other organizations involved in the supply chain for information systems or information system components related to the incident. system/product developers, integrators, manufacturers, packagers, assemblers, distributors, vendors, and resellers. Supply chain incidents include, for example, compromises/breaches involving information system components, information technology products, development processes or personnel, and distribution processes or warehousing facilities. Organizations determine the appropriate information to share considering the value gained from support by external organizations with the potential for harm due to sensitive information being released to outside organizations of perhaps questionable trustworthiness.	None
IR-7 **INCIDENT RESPONSE ASSISTANCE**	The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	None	Incident response support resources provided by organizations include, for example, help desks, assistance groups, and access to forensics services, when required. Related controls: AT-2, IR-4, IR-6, IR-8, SA-9.	(1) INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response-related information and support. Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support. (2) INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS The organization: (a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and (b) Identifies organizational incident response team members to the external providers. Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.	None
IR-8 **INCIDENT RESPONSE PLAN**	The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.	A.16.1.1	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.	None	None
IR-9 **INFORMATION SPILLAGE RESPONSE**	The organization responds to information spills by: a. Identifying the specific information involved in the information system contamination; b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; c. Isolating the contaminated information system or system component; d. Eradicating the information from the contaminated information system or component; e. Identifying other information systems or system components that may have been subsequently contaminated; and f. Performing other [Assignment: organization-defined actions].	None	Information spillage refers to instances where either classified or sensitive information is inadvertently placed on information systems that are not authorized to process such information. Such information spills often occur when information that is initially thought to be of lower sensitivity is transmitted to an information system and then is subsequently determined to be of higher sensitivity. At that point, corrective action is required. The nature of the organizational response is generally based upon the degree of sensitivity of the spilled information (e.g., security category or classification level), the security capabilities of the information system, the specific nature of contaminated storage media, and the access authorizations (e.g., security clearances) of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.	(1) INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills. (2) INFORMATION SPILLAGE RESPONSE | TRAINING The organization provides information spillage response training [Assignment: organization-defined frequency]. (3) INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions. Supplemental Guidance: Correction actions for information systems contaminated due to information spillages may be very time-consuming. During those periods, personnel may not have access to the contaminated systems, which may potentially affect their ability to conduct organizational business. (4) INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations. Supplemental Guidance: Security safeguards include, for example, making personnel exposed to spilled information aware of the federal laws, directives, policies, and/or regulations regarding the information and the restrictions imposed based on exposure to such information.	None
IR-10 **INTEGRATED INFORMATION SECURITY ANALYSIS TEAM**	The organization establishes an integrated team of forensic/malicious code analysts, tool developers, and real-time operations personnel.	None	Having an integrated team for incident response facilitates information sharing. Such capability allows organizational personnel, including developers, implementers, and operators, to leverage the team knowledge of the threat in order to implement defensive measures that will enable organizations to deter intrusions more effectively. Moreover, it promotes the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures. For example, when an intrusion is detected, the integrated security analysis team can rapidly develop an appropriate response for operators to implement, correlate the new incident with information on past intrusions, and augment ongoing intelligence development. This enables the team to identify adversary TTPs that are linked to the operations tempo or to specific missions/business functions, and to define responsive actions in a way that does not disrupt the mission/business operations. Ideally, information security analysis teams are distributed within organizations to make the capability more resilient.	None	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
MA-1 **SYSTEM MAINTENANCE POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and b. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and 2. System maintenance procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
MA-2 **CONTROLLED MAINTENANCE**	The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.	A.11.2.4 (only partially satisfies NIST control), A.11.2.5 (only partially satisfies NIST control)	This control addresses the information security aspects of the information system maintenance program and applies to all types of maintenance to any system component (including applications) conducted by any local or nonlocal entity (e.g., in-contract, warranty, in-house, software maintenance agreement). System maintenance also includes those components not directly associated with information processing and/or data/information retention such as scanners, copiers, and printers. Information necessary for creating effective maintenance records includes, for example: (i) date and time of maintenance; (ii) name of individuals or group performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) information system components/equipment removed or replaced (including identification numbers, if applicable). The level of detail included in maintenance records can be informed by the security categories of organizational information systems. Organizations consider supply chain issues associated with replacement components for information systems. Related controls: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.	(1) CONTROLLED MAINTENANCE | RECORD CONTENT [Withdrawn: Incorporated into MA-2]. (2) CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES The organization: (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (b) Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed. Supplemental Guidance: Related controls: CA-7, MA-3.	None
MA-3 **MAINTENANCE TOOLS**	The organization approves, controls, and monitors information system maintenance tools.	None	This control addresses security-related issues associated with maintenance tools used specifically for diagnostic and repair actions on organizational information systems. Maintenance tools can include hardware, software, and firmware items. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and subsequently into organizational information systems. Maintenance tools can include, for example, hardware/software diagnostic test equipment and hardware/software packet sniffers. This control does not cover hardware/software components that may support information system maintenance, yet are a part of the system, for example, the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch. Related controls: MA-2, MA-5, MP-6.	(1) MAINTENANCE TOOLS | INSPECT TOOLS The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. Supplemental Guidance: If, upon inspection of maintenance tools, organizations determine that the tools have been modified in an improper/unauthorized manner or contain malicious code, the incident is handled consistent with organizational policies and procedures for incident handling. Related control: SI-7. (2) MAINTENANCE TOOLS | INSPECT MEDIA The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system. Supplemental Guidance: If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with organizational incident handling policies and procedures. Related control: SI-3. (3) MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL The organization prevents the unauthorized removal of maintenance equipment containing organizational information by: (a) Verifying that there is no organizational information contained on the equipment; (b) Sanitizing or destroying the equipment; (c) Retaining the equipment within the facility; or (d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility. Supplemental Guidance: Organizational information includes all information specifically owned by organizations and information provided to organizations in which organizations serve as information stewards. (4) MAINTENANCE TOOLS | RESTRICTED TOOL USE The information system restricts the use of maintenance tools to authorized personnel only. Supplemental Guidance: This control enhancement applies to information systems that are used to carry out maintenance functions. Related controls: AC-2, AC-3, AC-5, AC-6.	None
MA-4 **NONLOCAL MAINTENANCE**	The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.	None	Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Authentication techniques used in the establishment of nonlocal maintenance and diagnostic sessions reflect the network access requirements in IA-2. Typically, strong authentication requires authenticators that are resistant to replay attacks and employ multifactor authentication. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, MP-6, PL-2, SC-7, SC-10, SC-17.	(1) NONLOCAL MAINTENANCE | AUDITING AND REVIEW The organization: (a) Audits nonlocal maintenance and diagnostic sessions [Assignment: organization-defined audit events]; and (b) Reviews the records of the maintenance and diagnostic sessions. Supplemental Guidance: Related controls: AU-2, AU-6, AU-12. (2) NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections. (3) NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION The organization: (a) Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or (b) Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system. Supplemental Guidance: Comparable security capability on information systems, diagnostic tools, and equipment providing maintenance services implies that the implemented security controls on those systems, tools, and equipment are at least as comprehensive as the controls on the information system being serviced. Related controls: MA-3, SA-12, SI-3, SI-7. (4) NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS The organization protects nonlocal maintenance sessions by: (a) Employing [Assignment: organization-defined authenticators that are replay resistant]; and (b) Separating the maintenance sessions from other network sessions with the information system by either: (1) Physically separated communications paths; or (2) Logically separated communications paths based upon encryption. Supplemental Guidance: Related control: SC-13. (5) NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS The organization: (a) Requires the approval of each nonlocal maintenance session by [Assignment: organization-defined personnel or roles]; and (b) Notifies [Assignment: organization-defined personnel or roles] of the date and time of planned nonlocal maintenance. Supplemental Guidance: Notification may be performed by maintenance personnel. Approval of nonlocal maintenance sessions is accomplished by organizational personnel with sufficient information security and information system knowledge to determine the appropriateness of the proposed maintenance. (6) NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications. Supplemental Guidance: Related controls: SC-8, SC-13. (7) NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION The information system implements remote disconnect verification at the termination of nonlocal maintenance and diagnostic sessions. Supplemental Guidance: Remote disconnect verification ensures that remote connections from nonlocal maintenance sessions have been terminated and are no longer available for use. Related control: SC-13.	None
MA-5 **MAINTENANCE PERSONNEL**	The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.	None	This control applies to individuals performing hardware or software maintenance on organizational information systems, while PE-2 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Technical competence of supervising individuals relates to the maintenance performed on the information systems while having required access authorizations refers to maintenance on and near the systems. Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, systems integrators, and consultants, may require privileged access to organizational information systems, for example, when required to conduct maintenance activities with little or no notice. Based on organizational assessments of risk, organizations may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for very limited time periods. Related controls: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.	(1) MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS The organization: (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; (2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and (b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems. Related controls: MP-6, PL-2. (2) MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for all compartments of information on the system. Supplemental Guidance: Related control: PS-3. (3) MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens. Supplemental Guidance: Related control: PS-3. (4) MAINTENANCE PERSONNEL | FOREIGN NATIONALS The organization ensures that: (a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on classified information systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and (b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified information systems are fully documented within Memoranda of Agreements. Supplemental Guidance: Related control: PS-3. (5) MAINTENANCE PERSONNEL | NONSYSTEM-RELATED MAINTENANCE The organization ensures that non-escorted personnel performing maintenance activities not directly associated with the information system but in the physical proximity of the system, have required access authorizations. Supplemental Guidance: Personnel performing maintenance activities in other capacities not directly related to the information system include, for example, physical plant personnel and janitorial personnel.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
MA-6 **TIMELY MAINTENANCE**	The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.	A.11.2.4	Organizations specify the information system components that result in increased risk to organizational operations and assets, individuals, other organizations, or the Nation when the functionality provided by those components is not operational. Organizational actions to obtain maintenance support typically include having appropriate contracts in place. Related controls: CM-8, CP-2, CP-7, SA-14, SA-15.	(1) TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE The organization performs preventive maintenance on [Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals]. Supplemental Guidance: Preventive maintenance includes proactive care and servicing of organizational information systems components for the purpose of maintaining equipment and facilities in satisfactory operating condition. Such maintenance provides for the systematic inspection, tests, measurements, adjustments, parts replacement, detection, and correction of incipient failures either before they occur or before they develop into major defects. The primary goal of preventive maintenance is to avoid/mitigate the consequences of equipment failures. Preventive maintenance is designed to preserve and restore equipment reliability by replacing worn components before they actually fail. Methods of determining what preventive (or other) failure management policies to apply include, for example, original equipment manufacturer (OEM) recommendations, statistical failure records, requirements of codes, legislation, or regulations within a jurisdiction, expert opinion, maintenance that has already been conducted on similar equipment, or measured values and performance indications. (2) TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE The organization performs predictive maintenance on [Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals]. Supplemental Guidance: Predictive maintenance, or condition-based maintenance, attempts to evaluate the condition of equipment by performing periodic or continuous (online) equipment condition monitoring. The goal of predictive maintenance is to perform maintenance at a scheduled point in time when the maintenance activity is most cost-effective and before the equipment loses performance within a threshold. The predictive component of predictive maintenance stems from the goal of predicting the future trend of the equipment's condition. This approach uses principles of statistical process control to determine at what point in the future maintenance activities will be appropriate. Most predictive maintenance inspections are performed while equipment is in service, thereby minimizing disruption of normal system operations. Predictive maintenance can result in substantial cost savings and higher system reliability. Predictive maintenance tends to include measurement of the item. To evaluate equipment condition, predictive maintenance utilizes nondestructive testing technologies such as infrared, acoustic (partial discharge and airborne ultrasonic), corona detection, vibration analysis, sound level measurements, oil analysis, and other specific online tests. (3) TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE The organization employs automated mechanisms to transfer predictive maintenance data to a computerized maintenance management system. Supplemental Guidance: A computerized maintenance management system maintains a computer database of information about the maintenance operations of organizations and automates processing equipment condition data in order to trigger maintenance planning, execution, and reporting.	None
MP-1 **MEDIA PROTECTION POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the MP family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
MP-2 **MEDIA ACCESS**	The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].	A.8.2.3, A.8.3.1, A.11.2.9	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.	(1) MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS [Withdrawn: Incorporated into MP-4 (2)]. (2) MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION [Withdrawn: Incorporated into SC-28 (1)].	None
MP-4 **MEDIA STORAGE**	The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	A.8.2.3, A.8.3.1, A.11.2.9	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Physically controlling information system media includes, for example, conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media. Secure storage includes, for example, a locked drawer, desk, or cabinet, or a controlled media library. The type of media storage is commensurate with the security category and/or classification of the information residing on the media. Controlled areas are areas for which organizations provide sufficient physical and procedural safeguards to meet the requirements established for protecting information and/or information systems. For media containing information determined by organizations to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls provide adequate protection. Related controls: CP-6, CP-9, MP-2, MP-7, PE-3.	(1) MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION [Withdrawn: Incorporated into SC-28 (1)]. (2) MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. Supplemental Guidance: Automated mechanisms can include, for example, keypads on the external entries to media storage areas. Related controls: AU-2, AU-9, AU-6, AU-12.	None
MP-7 **MEDIA USE**	The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].	A.8.2.3, A.8.3.1	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. This control also applies to mobile devices with information storage capability (e.g., smart phones, tablets, E-readers). In contrast to MP-2, which restricts user access to media, this control restricts the use of certain types of media on information systems, for example, restricting/prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical safeguards (e.g., policies, procedures, rules of behavior) to restrict the use of information system media. Organizations may restrict the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling/removing the ability to insert, read or write to such devices. Organizations may also limit the use of portable storage devices to only approved devices including, for example, devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may restrict the use of portable storage devices based on the type of device, for example, prohibiting the use of writeable, portable storage devices, and implementing this restriction by disabling or removing the capability to write to such devices. Related controls: AC-19, PL-4.	(1) MEDIA USE | PROHIBIT USE WITHOUT OWNER The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner. Supplemental Guidance: Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion). Related control: PL-4. (2) MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA The organization prohibits the use of sanitization-resistant media in organizational information systems. Supplemental Guidance: Sanitization-resistance applies to the capability to purge information from media. Certain types of media do not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media. Related control: MP-6.	None
MP-8 **MEDIA DOWNGRADING**	The organization: a. Establishes [Assignment: organization-defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization-defined strength and integrity]; b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c. Identifies [Assignment: organization-defined information system media requiring downgrading]; and d. Downgrades the identified information system media using the established process.	None	This control applies to all information system media, digital and non-digital, subject to release outside of the organization, whether or not the media is considered removable. The downgrading process, when applied to system media, removes information from the media, typically by security category or classification level, such that the information cannot be retrieved or reconstructed. Downgrading of media includes redacting information to enable wider release and distribution. Downgrading of media also ensures that empty space on the media (e.g., slack space within files) is devoid of information.	(1) MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS The organization documents information system media downgrading actions. Supplemental Guidance: Organizations can document the media downgrading process by providing information such as the downgrading technique employed, the identification number of the downgraded media, and the identity of the individual that authorized and/or performed the downgrading action. (2) MEDIA DOWNGRADING | EQUIPMENT TESTING The organization employs [Assignment: organization-defined tests] of downgrading equipment and procedures to verify correct performance [Assignment: organization-defined frequency]. (3) MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION The organization downgrades information system media containing [Assignment: organization-defined Controlled Unclassified Information (CUI)] prior to public release in accordance with applicable federal and organizational standards and policies. (4) MEDIA DOWNGRADING | CLASSIFIED INFORMATION The organization downgrades information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies. Supplemental Guidance: Downgrading of classified information uses approved sanitization tools, techniques, and procedures to transfer information confirmed to be unclassified from classified information systems to unclassified media.	None
PE-1 **PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PE family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
PE-2 **PHYSICAL ACCESS AUTHORIZATIONS**	The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Removes individuals from the facility access list when access is no longer required.	A.11.1.2 (only partially satisfies NIST control)	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal standards, policies, and procedures. This control only applies to areas within facilities that have not been designated as publicly accessible. Related controls: PE-3, PE-4, PS-3.	(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE The organization authorizes physical access to the facility where the information system resides based on position or role. Supplemental Guidance: Related controls: AC-2, AC-3, AC-6. (2) PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION The organization requires two forms of identification from [Assignment: organization-defined list of acceptable forms of identification] for visitor access to the facility where the information system resides. Supplemental Guidance: Acceptable forms of government photo identification include, for example, passports, Personal Identity Verification (PIV) cards, and drivers' licenses. In the case of gaining access to facilities using automated mechanisms, organizations may use PIV cards, key cards, PINs, and biometrics. Related controls: IA-2, IA-4, IA-5. (3) PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS The organization restricts unescorted access to the facility where the information system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined credentials]]. Supplemental Guidance: Due to the highly sensitive nature of classified information stored within certain facilities, it is important that individuals lacking sufficient security clearances, access approvals, or need to know, be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised. Related controls: PS-2, PS-6.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
PE-3 **PHYSICAL ACCESS CONTROL**	The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.	A.11.1.1, A.11.1.2, A.11.1.3	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.	(1) PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the information system]. Supplemental Guidance: This control enhancement provides additional physical security for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers). Related control: PS-2. (2) PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES The organization performs security checks [Assignment: organization-defined frequency] at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components. Supplemental Guidance: Organizations determine the extent, frequency, and/or randomness of security checks to adequately mitigate risk associated with exfiltration. Related controls: AC-4, SC-7. (3) PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING The organization employs guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week. Supplemental Guidance: Related controls: CP-6, CP-7. (4) PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS The organization uses lockable physical casings to protect [Assignment: organization-defined information system components] from unauthorized physical access. (5) PHYSICAL ACCESS CONTROL | TAMPER PROTECTION The organization employs [Assignment: organization-defined security safeguards] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the information system. Supplemental Guidance: Organizations may implement tamper detection/prevention at selected hardware components or tamper detection at some components and tamper prevention at other components. Tamper detection/prevention activities can employ many types of anti-tamper technologies including, for example, tamper-detection seals and anti-tamper coatings. Anti-tamper programs help to detect hardware alterations through counterfeiting and other supply chain-related risks. Related control: SA-12. (6) PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING The organization employs a penetration testing process that includes [Assignment: organization-defined frequency], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility. Supplemental Guidance: Related controls: CA-2, CA-7.	None
PE-4 **ACCESS CONTROL FOR TRANSMISSION MEDIUM**	The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].	A.11.1.2, A.11.2.3	Physical security safeguards applied to information system distribution and transmission lines help to prevent accidental damage, disruption, and physical tampering. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Security safeguards to control physical access to system distribution and transmission lines include, for example: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related controls: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.	None	None
PE-5 **ACCESS CONTROL FOR OUTPUT DEVICES**	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	A.11.1.2, A.11.1.3	Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by organizational personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices. Related controls: PE-2, PE-3, PE-4, PE-18.	(1) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS The organization: (a) Controls physical access to output from [Assignment: organization-defined output devices]; and (b) Ensures that only authorized individuals receive output from the device. Supplemental Guidance: Controlling physical access to selected output devices includes, for example, placing printers, copiers, and facsimile machines in controlled areas with keypad access controls or limiting access to individuals with certain types of badges. (2) ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY The information system: (a) Controls physical access to output from [Assignment: organization-defined output devices]; and (b) Links individual identity to receipt of the output from the device. Supplemental Guidance: Controlling physical access to selected output devices includes, for example, installing security functionality on printers, copiers, and facsimile machines that allows organizations to implement authentication (e.g., using a PIN or hardware token) on output devices prior to the release of output to individuals. (3) ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES The organization marks [Assignment: organization-defined information system output devices] indicating the appropriate security marking of the information permitted to be output from the device. Supplemental Guidance: Outputs devices include, for example, printers, monitors, facsimile machines, scanners, copiers, and audio devices. This control enhancement is generally applicable to information system output devices other than mobiles devices.	None
PE-6 **MONITORING PHYSICAL ACCESS**	The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.	None	Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.	(1) MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT The organization monitors physical intrusion alarms and surveillance equipment. (2) MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES The organization employs automated mechanisms to recognize [Assignment: organization-defined classes/types of intrusions] and initiate [Assignment: organization-defined response actions]. Supplemental Guidance: Related control: SI-4. (3) MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE The organization employs video surveillance of [Assignment: organization-defined operational areas] and retains video recordings for [Assignment: organization-defined time period]. Supplemental Guidance: This control enhancement focuses on recording surveillance video for purposes of subsequent review, if circumstances so warrant (e.g., a break-in detected by other means). It does not require monitoring surveillance video although organizations may choose to do so. Note that there may be legal considerations when performing and retaining video surveillance, especially if such surveillance is in a public location. (4) MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system]. Supplemental Guidance: This control enhancement provides additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers). Related controls: PS-2, PS-3.	None
PE-9 **POWER EQUIPMENT AND CABLING**	The organization protects power equipment and power cabling for the information system from damage and destruction.	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3	Organizations determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites. Related control: PE-4.	(1) POWER EQUIPMENT AND CABLING | REDUNDANT CABLING The organization employs redundant power cabling paths that are physically separated by [Assignment: organization-defined distance]. Supplemental Guidance: Physically separate, redundant power cables help to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged. (2) POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS The organization employs automatic voltage controls for [Assignment: organization-defined critical information system components].	None
PE-18 **LOCATION OF INFORMATION SYSTEM COMPONENTS**	The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.	A.8.2.3, A.11.1.4, A.11.2.1	Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and other forms of incoming electromagnetic radiation. In addition, organizations consider the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to information systems and therefore increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). Related controls: CP-2, PE-19, RA-3.	(1) LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy. Supplemental Guidance: Related control: PM-8.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
PL-1 **SECURITY PLANNING POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
PL-2 **SYSTEM SECURITY PLAN**	The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.	A.14.1.1	Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA 17.	(1) SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS [Withdrawn: Incorporated into PL-7]. (2) SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE [Withdrawn: Incorporated into PL-8]. (3) SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities. Supplemental Guidance: Security-related activities include, for example, security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing. Advance planning and coordination includes emergency and nonemergency (i.e., planned or nonurgent unplanned) situations. The process defined by organizations to plan and coordinate security-related activities can be included in security plans for information systems or other documents, as appropriate. Related controls: CP-4, IR-4.	None
PL-4 **RULES OF BEHAVIOR**	The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.	A.7.1.2, A.7.2.1, A.8.1.3	This control enhancement applies to organizational users. Organizations consider rules of behavior based on individual user roles and responsibilities, differentiating, for example, between rules that apply to privileged users and rules that apply to general users. Establishing rules of behavior for some types of non-organizational users including, for example, individuals who simply receive data/information from federal information systems, is often not feasible given the large number of such users and the limited nature of their interactions with the systems. Rules of behavior for both organizational and non-organizational users can also be established in AC-8, System Use Notification. PL-4 b. (the signed acknowledgment portion of this control) may be satisfied by the security awareness training and role-based security training programs conducted by organizations if such training includes rules of behavior. Organizations can use electronic signatures for acknowledging rules of behavior. Related controls: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.	(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites. Supplemental Guidance: This control enhancement addresses rules of behavior related to the use of social media/networking sites: (i) when organizational personnel are using such sites for official duties or in the conduct of official business; (ii) when organizational information is involved in social media/networking transactions; and (iii) when personnel are accessing social media/networking sites from organizational information systems. Organizations also address specific rules that prevent unauthorized entities from obtaining and/or inferring non-public organizational information (e.g., system account information, personally identifiable information) from social media/networking sites.	None
PL-7 **SECURITY CONCEPT OF OPERATIONS**	The organization: a. Develops a security Concept of Operations (CONOPS) for the information system containing at a minimum, how the organization intends to operate the system from the perspective of information security; and b. Reviews and updates the CONOPS [Assignment: organization-defined frequency].	A.14.1.1 (only partially satisfies NIST control)	The security CONOPS may be included in the security plan for the information system or in other system development life cycle-related documents, as appropriate. Changes to the CONOPS are reflected in ongoing updates to the security plan, the information security architecture, and other appropriate organizational documents (e.g., security specifications for procurements/acquisitions, system development life cycle documents, and systems/security engineering documents). Related control: PL-2.	None	None
PL-8 **INFORMATION SECURITY ARCHITECTURE**	The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.	A.14.1.1 (only partially satisfies NIST control)	This control addresses actions taken by organizations in the design and development of information systems. The information security architecture at the individual information system level is consistent with and complements the more global, organization-wide information security architecture described in PM-7 that is integral to and developed as part of the enterprise architecture. The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition, the security architecture can include other important security-related information, for example, user roles and access privileges assigned to each role, unique security requirements, the types of information processed, stored, and transmitted by the information system, restoration priorities of information and information system services, and any other specific protection needs. In today's modern architecture, it is becoming less common for organizations to control all information resources. There are going to be key dependencies on external information services and service providers. Describing such dependencies in the information security architecture is important to developing a comprehensive mission/business protection strategy. Establishing, developing, documenting, and maintaining under configuration control, a baseline configuration for organizational information systems is critical to implementing and maintaining an effective information security architecture. The development of the information security architecture is coordinated with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) to ensure that security controls needed to support privacy requirements are identified and effectively implemented. PL-8 is primarily directed at organizations (i.e., internally focused) to help ensure that organizations develop an information security architecture for the information system, and that the security architecture is integrated with or tightly coupled to the enterprise architecture through the organization-wide information security architecture. In contrast, SA-17 is primarily directed at external information technology product/system developers and integrators (although SA-17 could be used internally within organizations for in-house system development). SA-17, which is complementary to PL-8, is selected when organizations outsource the development of information systems or information system components to external entities, and there is a need to demonstrate/show consistency with the organization's enterprise architecture and information security architecture. Related controls: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17, Appendix J.	(1) INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH The organization designs its security architecture using a defense-in-depth approach that: (a) Allocates [Assignment: organization-defined security safeguards] to [Assignment: organization-defined locations and architectural layers]; and (b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner. Supplemental Guidance: Organizations strategically allocate security safeguards (procedural, technical, or both) in the security architecture so that adversaries have to overcome multiple safeguards to achieve their objective. Requiring adversaries to defeat multiple mechanisms makes it more difficult to successfully attack critical information resources (i.e., increases adversary work factor) and also increases the likelihood of detection. The coordination of allocated safeguards is essential to ensure that an attack that involves one safeguard does not create adverse unintended consequences (e.g., lockout, cascading alarms) by interfering with another safeguard. Placement of security safeguards is a key activity. Greater asset criticality or information value merits additional layering. Thus, an organization may choose to place anti-virus software at organizational boundary layers, email/web servers, notebook computers, and workstations to maximize the number of related safeguards adversaries must penetrate before compromising the information and information systems. Related controls: SC-29, SC-36. (2) INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY The organization requires that [Assignment: organization-defined security safeguards] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers. Supplemental Guidance: Different information technology products have different strengths and weaknesses. Providing a broad spectrum of products complements the individual offerings. For example, vendors offering malicious code protection typically update their products at different times, often developing solutions for known viruses, Trojans, or worms according to their priorities and development schedules. By having different products at different locations (e.g., server, boundary, desktop) there is an increased likelihood that at least one will detect the malicious code. Related control: SA-12.	None
PM-1 **INFORMATION SECURITY PROGRAM PLAN**	The organization: a. Develops and disseminates an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [Assignment: organization-defined frequency]; c. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and d. Protects the information security program plan from unauthorized disclosure and modification.	A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2	Information security program plans can be represented in single documents or compilations of documents at the discretion of organizations. The plans document the program management controls and organization-defined common controls. Information security program plans provide sufficient information about the program management controls/common controls (including specification of parameters for any assignment and selection statements either explicitly or by reference) to enable implementations that are unambiguously compliant with the intent of the plans and a determination of the risk to be incurred if the plans are implemented as intended. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.	None	None
PM-9 **RISK MANAGEMENT STRATEGY**	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; b. Implements the risk management strategy consistently across the organization; and c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.	None	An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.	None	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
PM-12 **INSIDER THREAT PROGRAM**	The organization implements an insider threat program that includes a cross-discipline insider threat incident handling team.	None	Organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. Insider threat programs include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns. A senior organizational official is designated by the department/agency head as the responsible individual to implement and provide oversight for the program. In addition to the centralized integration and analysis capability, insider threat programs as a minimum, prepare department/agency insider threat policies and implementation plans, conduct host-based user monitoring of individual employee activities on government-owned classified computers, provide insider threat awareness training to employees, receive access to information from all offices within the department/agency (e.g., human resources, legal, physical security, personnel security, information technology, information system security, and law enforcement) for insider threat analysis, and conduct self-assessments of department/agency insider threat posture. Insider threat programs can leverage the existence of incident handling teams organizations may already have in place, such as computer security incident response teams. Human resources records are especially important in this effort, as there is compelling evidence to show that some types of insider crimes are often preceded by nontechnical behaviors in the workplace (e.g., ongoing patterns of disgruntled behavior and conflicts with coworkers and other colleagues). These precursors can better inform and guide organizational officials in more focused, targeted monitoring efforts. The participation of a legal team is important to ensure that all monitoring activities are performed in accordance with appropriate legislation, directives, regulations, policies, standards, and guidelines. Related controls: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14.	None	None
PM-14 **TESTING, TRAINING, AND MONITORING**	The organization: a. Implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems: 1. Are developed and maintained; and 2. Continue to be executed in a timely manner; b. Reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.	None	This control ensures that organizations provide oversight for the security testing, training, and monitoring activities conducted organization-wide and that those activities are coordinated. With the importance of continuous monitoring programs, the implementation of information security across the three tiers of the risk management hierarchy, and the widespread use of common controls, organizations coordinate and consolidate the testing and monitoring activities that are routinely conducted as part of ongoing organizational assessments supporting a variety of security controls. Security training activities, while typically focused on individual information systems and specific roles, also necessitate coordination across all organizational elements. Testing, training, and monitoring plans and activities are informed by current threat and vulnerability assessments. Related controls: AT-3, CA-7, CP-4, IR-3, SI-4.	None	None
PM-15 **CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS**	The organization establishes and institutionalizes contact with selected groups and associations within the security community: a. To facilitate ongoing security education and training for organizational personnel; b. To maintain currency with recommended security practices, techniques, and technologies; and c. To share current security-related information including threats, vulnerabilities, and incidents.	A.6.1.4	Ongoing contact with security groups and associations is of paramount importance in an environment of rapidly changing technologies and threats. Security groups and associations include, for example, special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. Organizations select groups and associations based on organizational missions/business functions. Organizations share threat, vulnerability, and incident information consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related control: SI-5.	None	None
PM-16 **THREAT AWARENESS PROGRAM**	The organization implements a threat awareness program that includes a cross-organization information-sharing capability.	None	Because of the constantly changing and increasing sophistication of adversaries, especially the advanced persistent threat (APT), it is becoming more likely that adversaries may successfully breach or compromise organizational information systems. One of the best techniques to address this concern is for organizations to share threat information. This can include, for example, sharing threat events (i.e., tactics, techniques, and procedures) that organizations have experienced, mitigations that organizations have found are effective against certain types of threats, threat intelligence (i.e., indications and warnings about threats that are likely to occur). Threat information sharing may be bilateral (e.g., government-commercial cooperatives, government-government cooperatives), or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive requiring special agreements and protection, or less sensitive and freely shared. Related controls: PM-12, PM-16.	None	None
PS-1 **PERSONNEL SECURITY POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PS family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
RA-5 **VULNERABILITY SCANNING**	The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	A.12.6.1 (only partially satisfies NIST control)	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.	(1) VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY The organization employs vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned. Supplemental Guidance: The vulnerabilities to be scanned need to be readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This updating process helps to ensure that potential vulnerabilities in the information system are identified and addressed as quickly as possible. Related controls: SI-3, SI-7. (2) VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED The organization updates the information system vulnerabilities scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported]. Supplemental Guidance: Related controls: SI-3, SI-5. (3) VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE The organization employs vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked). (4) VULNERABILITY SCANNING | DISCOVERABLE INFORMATION The organization determines what information about the information system is discoverable by adversaries and subsequently takes [Assignment: organization-defined corrective actions]. Supplemental Guidance: Discoverable information includes information that adversaries could obtain without directly compromising or breaching the information system, for example, by collecting information the system is exposing or by conducting extensive searches of the web. Corrective actions can include, for example, notifying appropriate organizational personnel, removing designated information, or changing the information system to make designated information less relevant or attractive to adversaries. Related control: AU-13. (5) VULNERABILITY SCANNING | PRIVILEGED ACCESS The information system implements privileged access authorization to [Assignment: organization-identified information system components] for selected [Assignment: organization-defined vulnerability scanning activities]. Supplemental Guidance: In certain situations, the nature of the vulnerability scanning may be more intrusive or the information system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning. (6) VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. Supplemental Guidance: Related controls: IR-4, IR-5, SI-4. (7) VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS [Withdrawn: Incorporated into CM-8]. (8) VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited. Supplemental Guidance: Related control: AU-6. (9) VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES [Withdrawn: Incorporated into CA-8]. (10) VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	None
SA-1 **SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
SA-3 **SYSTEM DEVELOPMENT LIFE CYCLE**	The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6	A well-defined system development life cycle provides the foundation for the successful development, implementation, and operation of organizational information systems. To apply the required security controls within the system development life cycle requires a basic understanding of information security, threats, vulnerabilities, adverse impacts, and risk to critical missions/business functions. The security engineering principles in SA-8 cannot be properly applied if individuals that design, code, and test information systems and system components (including information technology products) do not understand security. Therefore, organizations include qualified personnel, for example, chief information security officers, security architects, security engineers, and information system security officers in system development life cycle activities to ensure that security requirements are incorporated into organizational information systems. It is equally important that developers include individuals on the development team that possess the requisite security expertise and skills to ensure that needed security capabilities are effectively integrated into the information system. Security awareness and training programs can help ensure that individuals having key security roles and responsibilities have the appropriate experience, skills, and expertise to conduct assigned system development life cycle activities. The effective integration of security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the system development life cycle and that those considerations are directly related to the organizational mission/business processes. This process also facilitates the integration of the information security architecture into the enterprise architecture, consistent with organizational risk management and information security strategies. Related controls: AT-3, PM-7, SA-8.	None	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SA-4 **ACQUISITION PROCESS**	The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2	Information system components are discrete, identifiable information technology assets (e.g., hardware, software, or firmware) that represent the building blocks of an information system. Information system components include commercial information technology products. Security functional requirements include security capabilities, security functions, and security mechanisms. Security strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to direct attack, and resistance to tampering or bypass. Security assurance requirements include: (i) development processes, procedures, practices, and methodologies; and (ii) evidence from development and assessment activities providing grounds for confidence that the required security functionality has been implemented and the required security strength has been achieved. Security documentation requirements address all phases of the system development life cycle. Security functionality, assurance, and documentation requirements are expressed in terms of security controls and control enhancements that have been selected through the tailoring process. The security control tailoring process includes, for example, the specification of parameter values through the use of assignment and selection statements and the specification of platform dependencies and implementation information. Security documentation provides user and administrator guidance regarding the implementation and operation of security controls. The level of detail required in security documentation is based on the security category or classification level of the information system and the degree to which organizations depend on the stated security capability, functions, or mechanisms to meet overall risk response expectations (as defined in the organizational risk management strategy). Security requirements can also include organizationally mandated configuration settings specifying allowed functions, ports, protocols, and services. Acceptance criteria for information systems, information system components, and information system services are defined in the same manner as such criteria for any organizational acquisition or procurement. The Federal Acquisition Regulation (FAR) Section 7.103 contains information security requirements from FISMA. Related controls: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.	(1) ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. Supplemental Guidance: Functional properties of security controls describe the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. Related control: SA-5. (2) ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail]. Supplemental Guidance: Organizations may require different levels of detail in design and implementation documentation for security controls employed in organizational information systems, system components, or information system services based on mission/business requirements, requirements for trustworthiness/resiliency, and requirements for analysis and testing. Information systems can be partitioned into multiple subsystems. Each subsystem within the system can contain one or more modules. The high-level design for the system is expressed in terms of multiple subsystems and the interfaces between subsystems providing security-relevant functionality. The low-level design for the system is expressed in terms of modules with particular emphasis on software and firmware (but not excluding hardware) and the interfaces between modules providing security-relevant functionality. Source code and hardware schematics are typically referred to as the implementation representation of the information system. Related control: SA-5. (3) ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES The organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [Assignment: organization-defined state-of-the-practice system/security engineering methods, software development methods, testing/evaluation/validation techniques, and quality control processes]. Supplemental Guidance: Following a well-defined system development life cycle that includes state-of-the-practice software development methods, systems/security engineering methods, quality control processes, and testing, evaluation, and validation techniques helps to reduce the number and severity of latent errors within information systems, system components, and information system services. Reducing the number/severity of such errors reduces the number of vulnerabilities in those systems, components, and services. Related control: SA-12. (4) ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS [Withdrawn: Incorporated into CM-8 (9)]. (5) ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS The organization requires the developer of the information system, system component, or information system service to: (a) Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and (b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade. Supplemental Guidance: Security configurations include, for example, the U.S. Government Configuration Baseline (USGCB) and any limitations on functions, ports, protocols, and services. Security characteristics include, for example, requiring that all default passwords have been changed. Related control: CM-8. (6) ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS The organization: (a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and (b) Ensures that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures. Supplemental Guidance: COTS IA or IA-enabled information technology products used to protect classified information by cryptographic means may be required to use NSA-approved key management. Related controls: SC-8, SC-12, SC-13. (7) ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES The organization:	None
SA-5 **INFORMATION SYSTEM DOCUMENTATION**	The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles].	A.12.1.1 (only partially satisfies NIST control)	This control helps organizational personnel understand the implementation and operation of security controls associated with information systems, system components, and information system services. Organizations consider establishing specific measures to determine the quality/completeness of the content provided. The inability to obtain needed documentation may occur, for example, due to the age of the information system/component or lack of support from developers and contractors. In those situations, organizations may need to recreate selected documentation if such documentation is essential to the effective implementation or operation of security controls. The level of protection provided for selected information system, component, or service documentation is commensurate with the security category or classification of the system. For example, documentation associated with a key DoD weapons system or command and control system would typically require a higher level of protection than a routine administrative system. Documentation that addresses information system vulnerabilities may also require an increased level of protection. Secure operation of the information system, includes, for example, initially starting the system and resuming secure system operation after any lapse in system operation. Related controls: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.	(1) INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS [Withdrawn: Incorporated into SA-4 (1)]. (2) INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES [Withdrawn: Incorporated into SA-4 (2)]. (3) INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN [Withdrawn: Incorporated into SA-4 (2)]. (4) INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN [Withdrawn: Incorporated into SA-4 (2)]. (5) INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE [Withdrawn: Incorporated into SA-4 (2)].	None
SA-8 **SECURITY ENGINEERING PRINCIPLES**	The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	A.14.2.5	Organizations apply security engineering principles primarily to new development information systems or systems undergoing major upgrades. For legacy systems, organizations apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems. Security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are trained on how to build secure software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. Related controls: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.	None	None
SA-9 **EXTERNAL INFORMATION SYSTEM SERVICES**	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2	External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.	(1) EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS The organization: (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and (b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services. Related controls: CA-6, RA-3. (2) EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES The organization requires providers of [Assignment: organization-defined external information system services] to identify the functions, ports, protocols, and other services required for the use of such services. Supplemental Guidance: Information from external service providers regarding the specific functions, ports, protocols, and services used in the provision of such services can be particularly useful when the need arises to understand the trade-offs involved in restricting certain functions/services or blocking certain ports/protocols. Related control: CM-7. (3) EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS The organization establishes, documents, and maintains trust relationships with external service providers based on [Assignment: organization-defined security requirements, properties, factors, or conditions defining acceptable trust relationships]. Supplemental Guidance: The degree of confidence that the risk from using external services is at an acceptable level depends on the trust that organizations place in the external providers, individually or in combination. Trust relationships can help organization to gain increased levels of confidence that participating service providers are providing adequate protection for the services rendered. Such relationships can be complicated due to the number of potential entities participating in the consumer-provider interactions, subordinate relationships and levels of trust, and the types of interactions between the parties. In some cases, the degree of trust is based on the amount of direct control organizations are able to exert on external service providers with regard to employment of security controls necessary for the protection of the service/information and the evidence brought forth as to the effectiveness of those controls. The level of control is typically established by the terms and conditions of the contracts or service-level agreements and can range from extensive control (e.g., negotiating contracts or agreements that specify security requirements for the providers) to very limited control (e.g., using contracts or service-level agreements to obtain commodity services such as commercial telecommunications services). In other cases, levels of trust are based on factors that convince organizations that required security controls have been employed and that determinations of control effectiveness exist. For example, separately authorized external information system services provided to organizations through well-established business relationships may provide degrees of trust in such services within the tolerable risk range of the organizations using the services. External service providers may also outsource selected services to other external entities, making the trust relationship more difficult and complicated to manage. Depending on the nature of the services, organizations may find it very difficult to place significant trust in external providers. This is not due to any inherent untrustworthiness on the part of providers, but to the intrinsic level of risk in the services. (4) EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests. Supplemental Guidance: As organizations increasingly use external service providers, the possibility exists that the interests of the service providers may diverge from organizational interests. In such situations, simply having the correct technical, procedural, or operational safeguards in place may not be sufficient if the service providers that implement and control those safeguards are not operating in a manner consistent with the interests of the consuming organizations. Possible actions that organizations might take to address such concerns include, for example, requiring background checks for selected service provider personnel, examining ownership records, employing only trustworthy service providers (i.e., providers with which organizations have had positive experiences), and conducting periodic/unscheduled visits to service provider facilities. (5) EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION The organization restricts the location of [Selection (one or more): information processing; information/data; information system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions]. Supplemental Guidance: The location of information processing, information/data storage, or information system services that are critical to organizations can have a direct impact on the ability of those organizations to successfully execute their missions/business functions. This situation exists when external providers control the location of processing, storage or services. The criteria external providers use for the selection of processing, storage, or service locations may be different from organizational criteria. For example, organizations may want to ensure that data/information storage locations are restricted to certain locations to facilitate incident	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SA-10 **DEVELOPER CONFIGURATION MANAGEMENT**	The organization requires the developer of the information system, system component, or information system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7	This control also applies to organizations conducting internal information systems development and integration. Organizations consider the quality and completeness of the configuration management activities conducted by developers as evidence of applying effective security safeguards. Safeguards include, for example, protecting from unauthorized modification or destruction, the master copies of all material used to generate security-relevant portions of the system hardware, software, and firmware. Maintaining the integrity of changes to the information system, information system component, or information system service requires configuration control throughout the system development life cycle to track authorized changes and prevent unauthorized changes. Configuration items that are placed under configuration management (if existence/use is required by other security controls) include: the formal model; the functional, high-level, and low-level design specifications; other design data; implementation documentation; source code and hardware schematics; the running version of the object code; tools for comparing new versions of security-relevant hardware descriptions and software/firmware source code with previous versions; and test fixtures and documentation. Depending on the mission/business needs of organizations and the nature of the contractual relationships in place, developers may provide configuration management support during the operations and maintenance phases of the life cycle. Related controls: CM-3, CM-4, CM-9, SA-12, SI-2.	(1) DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components. Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to software and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. Integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components. Related control: SI-7. (2) DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES The organization provides an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team. Supplemental Guidance: Alternate configuration management processes may be required, for example, when organizations use commercial off-the-shelf (COTS) information technology products. Alternate configuration management processes include organizational personnel that: (i) are responsible for reviewing/approving proposed changes to information systems, system components, and information system services; and (ii) conduct security impact analyses prior to the implementation of any changes to systems, components, or services (e.g., a configuration control board that considers security impacts of changes during development and includes representatives of both the organization and the developer, when applicable). (3) DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION The organization requires the developer of the information system, system component, or information system service to enable integrity verification of hardware components. Supplemental Guidance: This control enhancement allows organizations to detect unauthorized changes to hardware components through the use of tools, techniques, and/or mechanisms provided by developers. Organizations verify the integrity of hardware components, for example, with hard-to-copy labels and verifiable serial numbers provided by developers, and by requiring the implementation of anti-tamper technologies. Delivered hardware components also include updates to such components. Related control: SI-7. (4) DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION The organization requires the developer of the information system, system component, or information system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions and software/firmware source and object code with previous Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components between versions during development. In contrast, SA-10 (1) and SA-10 (3) allow organizations to detect unauthorized changes to hardware, software, and firmware components through the use of tools, techniques, and/or mechanisms provided by developers. (5) DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL The organization requires the developer of the information system, system component, or information system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version. Supplemental Guidance: This control enhancement addresses changes to hardware, software, and firmware components during initial development and during system life cycle updates. Maintaining the integrity between the master copies of security-relevant hardware, software, and firmware (including designs and source code) and the equivalent data in master copies on-site in operational environments is essential to ensure the availability of organizational information systems supporting critical missions and/or business functions. (6) DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION The organization requires the developer of the information system, system component, or information system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies. Supplemental Guidance: The trusted distribution of security-relevant hardware, software, and firmware updates helps to ensure that such updates are faithful representations of the master copies maintained by the developer and have not been tampered with during distribution.	None
SA-11 **DEVELOPER SECURITY TESTING AND EVALUATION**	The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.	A.14.2.7, A.14.2.8	Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.	(1) DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis. Supplemental Guidance: Static code analysis provides a technology and methodology for security reviews. Such analysis can be used to identify security vulnerabilities and enforce security coding practices. Static code analysis is most effective when used early in the development process, when each code change can be automatically scanned for potential weaknesses. Static analysis can provide clear remediation guidance along with defects to enable developers to fix such defects. Evidence of correct implementation of static analysis can include, for example, aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were fixed. An excessively high density of ignored findings (commonly referred to as ignored or false positives) indicates a potential problem with the analysis process or tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources. (2) DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service. Supplemental Guidance: Applications may deviate significantly from the functional and design specifications created during the requirements and design phases of the system development life cycle. Therefore, threat and vulnerability analyses of information systems, system components, and information system services prior to delivery are critical to the effective operation of those systems, components, and services. Threat and vulnerability analyses at this phase of the life cycle help to ensure that design or implementation changes have been accounted for, and that any new vulnerabilities created as a result of those changes have been reviewed and mitigated. Related controls: PM-15, RA-5. (3) DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE The organization: (a) Requires an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation; and (b) Ensures that the independent agent is either provided with sufficient information to complete the verification process or granted the authority to obtain such information. Supplemental Guidance: Independent agents have the necessary qualifications (i.e., expertise, skills, training, and experience) to verify the correct implementation of developer security assessment plans. Related controls: AT-3, CA-7, RA-5, SA-12. (4) DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS The organization requires the developer of the information system, system component, or information system service to perform a manual code review of [Assignment: organization-defined specific code] using [Assignment: organization-defined processes, procedures, and/or techniques]. Supplemental Guidance: Manual code reviews are usually reserved for the critical software and firmware components of information systems. Such code reviews are uniquely effective at identifying weaknesses that require knowledge of the application's requirements or context which are generally unavailable to more automated analytic tools and techniques such as static or dynamic analysis. Components benefiting from manual review include for example, verifying access control matrices against application controls and reviewing more detailed aspects of cryptographic implementations and controls. (5) DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING The organization requires the developer of the information system, system component, or information system service to perform penetration testing at [Assignment: organization-defined breadth/depth] and with [Assignment: organization-defined constraints]. Supplemental Guidance: Penetration testing is an assessment methodology in which assessors, using all available information technology product and/or information system documentation (e.g., product/system design specifications, source code, and administrator/operator manuals) and working under specific constraints, attempt to circumvent implemented security features of information technology products and information systems. Penetration testing can include, for example, white, gray, or black box testing with analyses performed by skilled security professionals simulating adversary actions. The objective of penetration testing is to uncover potential vulnerabilities in information technology products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. Penetration tests can be performed in conjunction with automated and manual code reviews to provide greater levels of analysis than would ordinarily be possible. (6) DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS	None
SA-12 **SUPPLY CHAIN PROTECTION**	The organization protects against supply chain threats to the information system, system component, or information system service by employing [Assignment: organization-defined security safeguards] as part of a comprehensive, defense-in-breadth information security strategy.	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3	Information systems (including system components that compose those systems) need to be protected throughout the system development life cycle (i.e., during design, development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Protection of organizational information systems is accomplished through threat awareness, by the identification, management, and reduction of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to respond to risk. Organizations consider implementing a standardized process to address supply chain risk with respect to information systems and system components, and to educate the acquisition workforce on threats, risk, and required security controls. Organizations use the acquisition/procurement processes to require supply chain entities to implement necessary security safeguards to: (i) reduce the likelihood of unauthorized modifications at each stage in the supply chain; and (ii) protect information systems and information system components, prior to taking delivery of such systems/components. This control also applies to information system services. Security safeguards include, for example: (i) security controls for development systems, development facilities, and external connections to development systems; (ii) vetting development personnel; and (iii) use of tamper-evident packaging during shipping/warehousing. Methods for reviewing and protecting development plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18, SA-19, SC-29, SC-30, SC-38, SI-7.	(1) SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS The organization employs [Assignment: organization-defined tailored acquisition strategies, contract tools, and procurement methods] for the purchase of the information system, system component, or information system service from suppliers. Supplemental Guidance: The use of acquisition and procurement processes by organizations early in the system development life cycle provides an important vehicle to protect the supply chain. Organizations use available all-source intelligence analysis to inform the tailoring of acquisition strategies, tools, and methods. There are a number of different tools and techniques available (e.g., obscuring the end use of an information system or system component, using blind or filtered buys). Organizations also consider creating incentives for suppliers who: (i) implement required security safeguards; (ii) promote transparency into their organizational processes and security practices; (iii) provide additional vetting of the processes and security practices of subordinate suppliers, critical information system components, and services; (iv) restrict purchases from specific suppliers or countries; and (v) provide contract language regarding the prohibition of tainted or counterfeit components. In addition, organizations consider minimizing the time between purchase decisions and required delivery to limit opportunities for adversaries to corrupt information system components or products. Finally, organizations can use trusted/controlled distribution, delivery, and warehousing options to reduce supply chain risk (e.g., requiring tamper-evident packaging of information system components during shipping and warehousing). Related control: SA-19. (2) SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS The organization conducts a supplier review prior to entering into a contractual agreement to acquire the information system, system component, or information system service. Supplemental Guidance: Supplier reviews include, for example: (i) analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and (ii) assessment of supplier training and experience in developing systems, components, or services with the required security capability. These reviews provide organizations with increased levels of visibility into supplier activities during the system development life cycle to promote more effective supply chain risk management. Supplier reviews can also help to determine whether primary suppliers have security safeguards in place and a practice for vetting subordinate suppliers, for example, second- and third-tier suppliers, and any subcontractors. (3) SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING [Withdrawn: Incorporated into SA-12 (1)]. (4) SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS [Withdrawn: Incorporated into SA-12 (13)]. (5) SUPPLY CHAIN PROTECTION | LIMITATION OF HARM The organization employs [Assignment: organization-defined security safeguards] to limit harm from potential adversaries identifying and targeting the organizational supply chain. Supplemental Guidance: Supply chain risk is part of the advanced persistent threat (APT). Security safeguards and countermeasures to reduce the probability of adversaries successfully identifying and targeting the supply chain include, for example: (i) avoiding the purchase of custom configurations to reduce the risk of acquiring information systems, components, or products that have been corrupted via supply chain actions targeted at specific organizations; (ii) employing a diverse set of suppliers to limit the potential harm from any given supplier in the supply chain; (iii) employing approved vendor lists with standing reputations in industry, and (iv) using procurement carve outs (i.e., exclusions to commitments or obligations). (6) SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME [Withdrawn: Incorporated into SA-12 (1)]. (7) SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE The organization conducts an assessment of the information system, system component, or information system service prior to selection, acceptance, or update. Supplemental Guidance: Assessments include, for example, testing, evaluations, reviews, and analyses. Independent, third-party entities or organizational personnel conduct assessments of systems, components, products, tools, and services. Organizations conduct assessments to uncover unintentional vulnerabilities and intentional vulnerabilities including, for example, malicious code, malicious processes, defective software, and counterfeits. Assessments can include, for example, static analyses, dynamic analyses, simulations, white, gray, and black box testing, fuzz testing, penetration testing, and ensuring that components or services are genuine (e.g., using tags, cryptographic hash verifications, or digital signatures). Evidence generated during security assessments is documented for follow-on actions carried out by organizations. Related controls: CA-2, SA-11. (8) SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE The organization uses all-source intelligence analysis of suppliers and potential suppliers of the information system, system component, or information system service.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SA-13 **TRUSTWORTHINESS**	The organization: a. Describes the trustworthiness required in the [Assignment: organization-defined information system, information system component, or information system service] supporting its critical missions/business functions; and b. Implements [Assignment: organization-defined assurance overlay] to achieve such trustworthiness.	None	This control helps organizations to make explicit trustworthiness decisions when designing, developing, and implementing information systems that are needed to conduct critical organizational missions/business functions. Trustworthiness is a characteristic/property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information it processes, stores, or transmits. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of risk despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Trustworthy systems are important to mission/business success. Two factors affecting the trustworthiness of information systems include: (i) security functionality (i.e., the security features, functions, and/or mechanisms employed within the system and its environment of operation); and (ii) security assurance (i.e., the grounds for confidence that the security functionality is effective in its application). D evelopers, implementers, operators, and maintainers of organizational information systems can increase the level of assurance (and trustworthiness), for example, by employing well-defined security policy models, structured and rigorous hardware, software, and firmware development techniques, sound system/security engineering principles, and secure configuration settings (defined by a set of assurance-related security controls in Appendix E). Assurance is also based on the assessment of evidence produced during the system development life cycle. Critical missions/business functions are supported by high-impact systems and the associated assurance requirements for such systems. The additional assurance controls in Table E-4 in Appendix E (designated as optional) can be used to develop and implement high-assurance solutions for specific information systems and system components using the concept of overlays described in Appendix I. Organizations select assurance overlays that have been developed, validated, and approved for community adoption (e.g., cross-organization, governmentwide), limiting the development of such overlays on an organization-by-organization basis. Organizations can conduct criticality analyses as described in SA-14, to determine the information systems, system components, or information system services that require high-assurance solutions. Trustworthiness requirements and assurance overlays can be described in the security plans for organizational information systems. Related controls: RA-2, SA-4, SA-8, SA-14, SC-3.	None	None
SA-14 **CRITICALITY ANALYSIS**	The organization identifies critical information system components and functions by performing a criticality analysis for [Assignment: organization-defined information systems, information system components, or information system services] at [Assignment: organization-defined decision points in the system development life cycle].	None	Criticality analysis is a key tenet of supply chain risk management and informs the prioritization of supply chain protection activities such as attack surface reduction, use of all-source intelligence, and tailored acquisition strategies. Information system engineers can conduct an end-to-end functional decomposition of an information system to identify mission-critical functions and components. The functional decomposition includes the identification of core organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and beyond the information system boundary. Information system components that allow for unmediated access to critical components or functions are considered critical due to the inherent vulnerabilities such components create. Criticality is assessed in terms of the impact of the function or component failure on the ability of the component to complete the organizational missions supported by the information system. A criticality analysis is performed whenever an architecture or design is being developed or modified, including upgrades. Related controls: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.	(1) CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING [Withdrawn: Incorporated into SA-20].	None
SA-15 **DEVELOPMENT PROCESS, STANDARDS, AND TOOLS**	The organization: a. Requires the developer of the information system, system component, or information system service to follow a documented development process that: 1. Explicitly addresses security requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Reviews the development process, standards, tools, and tool options/configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [Assignment: organization-defined security requirements].	A.6.1.5, A.14.2.1	Development tools include, for example, programming languages and computer-aided design (CAD) systems. Reviews of development processes can include, for example, the use of maturity models to determine the potential effectiveness of such processes. Maintaining the integrity of changes to tools and processes enables accurate supply chain risk assessment and mitigation, and requires robust configuration control throughout the life cycle (including design, development, transport, delivery, integration, and maintenance) to track authorized changes and prevent unauthorized changes. Related controls: SA-3, SA-8.	(1) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS The organization requires the developer of the information system, system component, or information system service to: (a) Define quality metrics at the beginning of the development process; and (b) Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery]. Supplemental Guidance: Organizations use quality metrics to establish minimum acceptable levels of information system quality. Metrics may include quality gates which are collections of completion criteria or sufficiency standards representing the satisfactory execution of particular phases of the system development project. A quality gate, for example, may require the elimination of all compiler warnings or an explicit determination that the warnings have no impact on the effectiveness of required security capabilities. During the execution phases of development projects, quality gates provide clear, unambiguous indications of progress. Other metrics apply to the entire development project. These metrics can include defining the severity thresholds of vulnerabilities, for example, requiring no known vulnerabilities in the delivered information system with a Common Vulnerability Scoring System (CVSS) severity of Medium or High. (2) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS The organization requires the developer of the information system, system component, or information system service to select and employ a security tracking tool for use during the development process. Supplemental Guidance: Information system development teams select and deploy security tracking tools, including, for example, vulnerability/work item tracking systems that facilitate assignment, sorting, filtering, and tracking of completed work items or tasks associated with system development processes. (3) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS The organization requires the developer of the information system, system component, or information system service to perform a criticality analysis at [Assignment: organization-defined breadth/depth] and at [Assignment: organization-defined decision points in the system development life cycle]. Supplemental Guidance: This control enhancement provides developer input to the criticality analysis performed by organizations in SA-14. Developer input is essential to such analysis because organizations may not have access to detailed design documentation for information system components that are developed as commercial off-the-shelf (COTS) information technology products (e.g., functional specifications, high-level designs, low-level designs, and source code/hardware schematics). Related controls: SA-4, SA-14. (4) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS The organization requires that developers perform threat modeling and a vulnerability analysis for the information system at [Assignment: organization-defined breadth/depth] that: (a) Uses [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]; (b) Employs [Assignment: organization-defined tools and methods]; and (c) Produces evidence that meets [Assignment: organization-defined acceptance criteria]. Supplemental Guidance: Related control: SA-4. (5) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION The organization requires the developer of the information system, system component, or information system service to reduce attack surfaces to [Assignment: organization-defined thresholds]. Supplemental Guidance: Attack surface reduction is closely aligned with developer threat and vulnerability analyses and information system architecture and design. Attack surface reduction is a means of reducing risk to organizations by giving attackers less opportunity to exploit weaknesses or deficiencies (i.e., potential vulnerabilities) within information systems, information system components, and information system services. Attack surface reduction includes, for example, applying the principle of least privilege, employing layered defenses, applying the principle of least functionality (i.e., restricting ports, protocols, functions, and services), deprecating unsafe functions, and eliminating application programming interfaces (APIs) that are vulnerable to cyber attacks. Related control: CM-7. (6) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT The organization requires the developer of the information system, system component, or information system service to implement an explicit process to continuously improve the development process. Supplemental Guidance: Developers of information systems, information system components, and information system services consider the effectiveness/efficiency of current development processes for meeting quality objectives and addressing security capabilities in current threat environments. (7) DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS	None
SA-16 **DEVELOPER-PROVIDED TRAINING**	The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.	None	This control applies to external and internal (in-house) developers. Training of personnel is an essential element to ensure the effectiveness of security controls implemented within organizational information systems. Training options include, for example, classroom-style training, web-based/computer-based training, and hands-on training. Organizations can also request sufficient training materials from developers to conduct in-house training or offer self-training to organizational personnel. Organizations determine the type of training necessary and may require different types of training for different security functions, controls, or mechanisms. Related controls: AT-2, AT-3, SA-5.	None	None
SA-17 **DEVELOPER SECURITY ARCHITECTURE AND DESIGN**	The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.	A.14.2.1, A.14.2.5	This control is primarily directed at external developers, although it could also be used for internal (in-house) development. In contrast, PL-8 is primarily directed at internal developers to help ensure that organizations develop an information security architecture and such security architecture is integrated or tightly coupled to the enterprise architecture. This distinction is important if/when organizations outsource the development of information systems, information system components, or information system services to external entities, and there is a requirement to demonstrate consistency with the organization's enterprise architecture and information security architecture. Related controls: PL-8, PM-7, SA-3, SA-8.	(1) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL The organization requires the developer of the information system, system component, or information system service to: (a) Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security policy] to be enforced; and (b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented. Supplemental Guidance: Formal models describe specific behaviors or security policies using formal languages, thus enabling the correctness of those behaviors/policies to be formally proven. Not all components of information systems can be modeled, and generally, formal specifications are scoped to specific behaviors or policies of interest (e.g., nondiscretionary access control policies). Organizations choose the particular formal modeling language and approach based on the nature of the behaviors/policies to be described and the available tools. Formal modeling tools include, for example, Gypsy and Zed. (2) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS The organization requires the developer of the information system, system component, or information system service to: (a) Define security-relevant hardware, software, and firmware; and (b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete. Supplemental Guidance: Security-relevant hardware, software, and firmware represent the portion of the information system, component, or service that must be trusted to perform correctly in order to maintain required security properties. Related control: SA-5. (3) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE The organization requires the developer of the information system, system component, or information system service to: (a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model; (c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and (e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware. Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or implementation details present have no impact on the behaviors or policies being modeled. Formal methods can be used to show that the high-level security properties are satisfied by the formal information system description, and that the formal system description is correctly implemented by a description of some lower level, for example a hardware description. Consistency between the formal top-level specification and the formal policy models is generally not amenable to being fully proven. Therefore, a combination of formal/informal methods may be needed to show such consistency. Consistency between the formal top-level specification and the implementation may require the use of an informal demonstration due to limitations in the applicability of formal methods to prove that the specification accurately reflects the implementation. Hardware, software, and firmware mechanisms strictly internal to security-relevant hardware, software, and firmware 5. (4) DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE The organization requires the developer of the information system, system component, or information system service to: (a) Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; (b) Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model; (c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; (d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and (e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware. Supplemental Guidance: Correspondence is an important part of the assurance gained through modeling. It demonstrates that the implementation is an accurate transformation of the model, and that any additional code or	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SA-18 **TAMPER RESISTANCE AND DETECTION**	The organization implements a tamper protection program for the information system, system component, or information system service.	None	Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use. Related controls: PE-3, SA-12, SI-7.	(1) TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance. Supplemental Guidance: Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. Customization of information systems and system components can make substitutions easier to detect and therefore limit damage. Related control: SA-3. (2) TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES The organization inspects [Assignment: organization-defined information systems, system components, or devices] [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering. Supplemental Guidance: This control enhancement addresses both physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of need for inspection include, for example, when individuals return from travel to high-risk locations. Related control: SI-4.	None
SA-21 **DEVELOPER SCREENING**	The organization requires that the developer of [Assignment: organization-defined information system, system component, or information system service]: a. Have appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and b. Satisfy [Assignment: organization-defined additional personnel screening criteria].	A.7.1.1	Because the information system, system component, or information system service may be employed in critical activities essential to the national and/or economic security interests of the United States, organizations have a strong interest in ensuring that the developer is trustworthy. The degree of trust required of the developer may need to be consistent with that of the individuals accessing the information system/component/service once deployed. Examples of authorization and personnel screening criteria include clearance, satisfactory background checks, citizenship, and nationality. Trustworthiness of developers may also include a review and analysis of company ownership and any relationships the company has with entities potentially affecting the quality/reliability of the systems, components, or services being developed. Related controls: PS-3, PS-7.	(1) DEVELOPER SCREENING | VALIDATION OF SCREENING The organization requires the developer of the information system, system component, or information system service take [Assignment: organization-defined actions] to ensure that the required access authorizations and screening criteria are satisfied. Supplemental Guidance: Satisfying required access authorizations and personnel screening criteria includes, for example, providing a listing of all the individuals authorized to perform development activities on the selected information system, system component, or information system service so that organizations can validate that the developer has satisfied the necessary authorization and screening requirements.	None
SC-1 **SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
SC-7 **BOUNDARY PROTECTION**	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.	(1) BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS [Withdrawn: Incorporated into SC-7]. (2) BOUNDARY PROTECTION | PUBLIC ACCESS [Withdrawn: Incorporated into SC-7]. (3) BOUNDARY PROTECTION | ACCESS POINTS The organization limits the number of external network connections to the information system. Supplemental Guidance: Limiting the number of external network connections facilitates more comprehensive monitoring of inbound and outbound communications traffic. The Trusted Internet Connection (TIC) initiative is an example of limiting the number of external network connections. (4) BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Protects the confidentiality and integrity of the information being transmitted across each interface; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. Supplemental Guidance: Related control: SC-8. (5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION The information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed. (6) BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES [Withdrawn: Incorporated into SC-7 (18)]. (7) BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks. Supplemental Guidance: This control enhancement is implemented within remote devices (e.g., notebook computers) through configuration settings to disable split tunneling in those devices, and by preventing those configuration settings from being readily configurable by users. This control enhancement is implemented within the information system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling. Split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling. (8) BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces. Supplemental Guidance: External networks are networks outside of organizational control. A proxy server is a server (i.e., information system or application) that acts as an intermediary for clients requesting information system resources (e.g., files, connections, web pages, or services) from other organizational servers. Client requests established through an initial connection to the proxy server are evaluated to manage complexity and to	None
SC-8 **TRANSMISSION CONFIDENTIALITY AND INTEGRITY**	The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information.	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.	(1) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION The information system implements cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13. (2) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING The information system maintains the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception. Supplemental Guidance: Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example, during aggregation, at protocol transformation points, and during packing/unpacking. These unauthorized disclosures or modifications compromise the confidentiality or integrity of the information. Related control: AU-10. (3) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS The information system implements cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Message externals include, for example, message headers/routing information. This control enhancement prevents the exploitation of message externals and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Header/routing information is sometimes transmitted unencrypted because the information is not properly identified by organizations as having significant value costs. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13. (4) TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS The information system implements cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical safeguards]. Supplemental Guidance: This control enhancement addresses protection against unauthorized disclosure of information. Communication patterns include, for example, frequency, periods, amount, and predictability. Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to missions/business functions supported by organizational information systems. This control enhancement prevents the derivation of intelligence based on communications patterns and applies to both internal and external networks or links that may be visible to individuals who are not authorized users. Encrypting the links and transmitting in continuous, fixed/random patterns prevents the derivation of intelligence from the system communications patterns. Alternative physical safeguards include, for example, protected distribution systems. Related controls: SC-12, SC-13.	None
SC-12 **CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**	The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].	A.10.1.2	Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance, specifying appropriate options, levels, and parameters. Organizations manage trust stores to ensure that only approved trust anchors are in such trust stores. This includes certificates with visibility external to organizational information systems and certificates related to the internal operations of systems. Related controls: SC-13, SC-17.	(1) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY The organization maintains availability of information in the event of the loss of cryptographic keys by users. Supplemental Guidance: Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys (e.g., due to forgotten passphrase). (2) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS The organization produces, controls, and distributes symmetric cryptographic keys using [Selection: NIST FIPS-compliant; NSA-approved] key management technology and processes. (3) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key]. (4) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES [Withdrawn: Incorporated into SC-12]. (5) CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS [Withdrawn: Incorporated into SC-12].	The corporate PKI solution should be used where applicable. Consult with the Product Security Head or PKI certificate policy owner to get the latest certificate policy (CP).

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SC-13 **CRYPTOGRAPHIC PROTECTION**	The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5	Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.	(1) CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY [Withdrawn: Incorporated into SC-13]. (2) CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY [Withdrawn: Incorporated into SC-13]. (3) CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS [Withdrawn: Incorporated into SC-13]. (4) CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES [Withdrawn: Incorporated into SC-13].	None
SC-17 **PUBLIC KEY INFRASTRUCTURE CERTIFICATES**	The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.	A.10.1.2	For all certificates, organizations manage information system trust stores to ensure only approved trust anchors are in the trust stores. This control addresses both certificates with visibility external to organizational information systems and certificates related to the internal operations of systems, for example, application-specific time services. Related control: SC-12.	None	The corporate PKI solution should be used where applicable. Consult with the Product Security Head or PKI certificate policy owner to get the latest certificate policy (CP).
SC-25 **THIN NODES**	The organization employs [Assignment: organization-defined information system components] with minimal functionality and information storage.	None	The deployment of information system components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber attacks. Related control: SC-30.	None	None
SC-26 **HONEYPOTS**	The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.	None	A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function. Depending upon the specific usage of the honeypot, consultation with the Office of the General Counsel before deployment may be needed. Related controls: SC-30, SC-44, SI-3, SI-4.	None. (1) HONEYPOTS | DETECTION OF MALICIOUS CODE [Withdrawn: Incorporated into SC-35].	None
SC-28 **PROTECTION OF INFORMATION AT REST**	The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest].	A.8.2.3 (only partially satisfies NIST control)	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.	(1) PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [Assignment: organization-defined information system components]. Supplemental Guidance: Selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of organizational information. The strength of mechanism is commensurate with the security category and/or classification of the information. This control enhancement applies to significant concentrations of digital media in organizational areas designated for media storage and also to limited quantities of media generally associated with information system components in operational environments (e.g., portable storage devices, mobile devices). Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields). Organizations employing cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions. Related controls: AC-19, SC-12. (2) PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE The organization removes from online storage and stores off-line in a secure location [Assignment: organization-defined information]. Supplemental Guidance: Removing organizational information from online information system storage to off-line storage eliminates the possibility of individuals gaining unauthorized access to the information through a network. Therefore, organizations may choose to move information to off-line storage in lieu of protecting such information in online storage.	None
SC-29 **HETEROGENEITY**	The organization employs a diverse set of information technologies for [Assignment: organization-defined information system components] in the implementation of the information system.	None	Increasing the diversity of information technologies within organizational information systems reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one information system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations. Related controls: SA-12, SA-14, SC-27.	(1) HETEROGENEITY | VIRTUALIZATION TECHNIQUES The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency]. Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes can result in an increased work factor for adversaries in order to carry out successful cyber attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems/applications, provide virtual changes that impede attacker success while reducing configuration management efforts. In addition, virtualization techniques can assist organizations in isolating untrustworthy software and/or software of dubious provenance into confined execution environments.	None
SC-30 **CONCEALMENT AND MISDIRECTION**	The organization employs [Assignment: organization-defined concealment and misdirection techniques] for [Assignment: organization-defined information systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries.	None	Concealment and misdirection techniques can significantly reduce the targeting capability of adversaries (i.e., window of opportunity and available attack surface) to initiate and complete cyber attacks. For example, virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Increased use of concealment/misdirection techniques including, for example, randomness, uncertainty, and virtualization, may sufficiently confuse and mislead adversaries and subsequently increase the risk of discovery and/or exposing tradecraft. Concealment/misdirection techniques may also provide organizations additional time to successfully perform core missions and business functions. Because of the time and effort required to support concealment/misdirection techniques, it is anticipated that such techniques would be used by organizations on a very limited basis. Related controls: SC-26, SC-29, SI-14.	(1) CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES [Withdrawn: Incorporated into SC-29 (1)]. (2) CONCEALMENT AND MISDIRECTION | RANDOMNESS The organization employs [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets. Supplemental Guidance: Randomness introduces increased levels of uncertainty for adversaries regarding the actions organizations take in defending against cyber attacks. Such actions may impede the ability of adversaries to correctly target information resources of organizations supporting critical missions/business functions. Uncertainty may also cause adversaries to hesitate before initiating or continuing attacks. Misdirection techniques involving randomness include, for example, performing certain routine actions at different times of day, employing different information technologies (e.g., browsers, search engines), using different suppliers, and rotating roles and responsibilities of organizational personnel. (3) CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS The organization changes the location of [Assignment: organization-defined processing and/or storage] [Selection: [Assignment: organization-defined time frequency]; at random time intervals]]. Supplemental Guidance: Adversaries target critical organizational missions/business functions and the information resources supporting those missions and functions while at the same time, trying to minimize exposure of their existence and tradecraft. The static, homogeneous, and deterministic nature of organizational information systems targeted by adversaries, make such systems more susceptible to cyber attacks with less adversary cost and effort to be successful. Changing organizational processing and storage locations (sometimes referred to as moving target defense) addresses the advanced persistent threat (APT) using techniques such as virtualization, distributed processing, and replication. This enables organizations to relocate the information resources (i.e., processing and/or storage) supporting critical missions and business functions. Changing locations of processing activities and/or storage sites introduces uncertainty into the targeting activities by adversaries. This uncertainty increases the work factor of adversaries making compromises or breaches to organizational information systems much more difficult and time-consuming, and increases the chances that adversaries may inadvertently disclose aspects of tradecraft while attempting to locate critical organizational resources. (4) CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION The organization employs realistic, but misleading information in [Assignment: organization-defined information system components] with regard to its security state or posture. Supplemental Guidance: This control enhancement misleads potential adversaries regarding the nature and extent of security safeguards deployed by organizations. As a result, adversaries may employ incorrect (and as a result ineffective) attack techniques. One way of misleading adversaries is for organizations to place misleading information regarding the specific security controls deployed in external information systems that are known to be accessed or targeted by adversaries. Another technique is the use of deception nets (e.g., honeynets, virtualized environments) that mimic actual aspects of organizational information systems but use, for example, out-of-date software configurations. (5) CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS The organization employs [Assignment: organization-defined techniques] to hide or conceal [Assignment: organization-defined information system components]. Supplemental Guidance: By hiding, disguising, or otherwise concealing critical information system components, organizations may be able to decrease the probability that adversaries target and successfully compromise those assets. Potential means for organizations to hide and/or conceal information system components include, for example, configuration of routers or the use of honeynets or virtualization techniques.	None
SC-31 **COVERT CHANNEL ANALYSIS**	The organization: a. Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and b. Estimates the maximum bandwidth of those channels.	None	Developers are in the best position to identify potential areas within systems that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by organizations). Covert channel analysis is also meaningful for multilevel secure (MLS) information systems, multiple security level (MSL) systems, and cross-domain systems. Related controls: AC-3, AC-4, PL-2.	(1) COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY The organization tests a subset of the identified covert channels to determine which channels are exploitable. (2) COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH The organization reduces the maximum bandwidth for identified covert [Selection (one or more); storage; timing] channels to [Assignment: organization-defined values]. Supplemental Guidance: Information system developers are in the best position to reduce the maximum bandwidth for identified covert storage and timing channels. (3) COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS The organization measures the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the information system. Supplemental Guidance: This control enhancement addresses covert channel bandwidth in operational environments versus developmental environments. Measuring covert channel bandwidth in operational environments helps organizations to determine how much information can be covertly leaked before such leakage adversely affects organizational missions/business functions. Covert channel bandwidth may be significantly different when measured in those settings that are independent of the particular environments of operation (e.g., laboratories or development environments).	None
SC-34 **NON-MODIFIABLE EXECUTABLE PROGRAMS**	The information system at [Assignment: organization-defined information system components]: a. Loads and executes the operating environment from hardware-enforced, read-only media; and b. Loads and executes [Assignment: organization-defined applications] from hardware-enforced, read-only media.	None	The term operating environment is defined as the specific code that hosts applications, for example, operating systems, executives, or monitors including virtual machine monitors (i.e., hypervisors). It can also include certain applications running directly on hardware platforms. Hardware-enforced, read-only media include, for example, Compact Disk-Recordable (CD-R)/Digital Video Disk-Recordable (DVD-R) disk drives and one-time programmable read-only memory. The use of non-modifiable storage ensures the integrity of software from the point of creation of the read-only image. The use of reprogrammable read-only memory can be accepted as read-only media provided: (i) integrity can be adequately protected from the point of initial writing to the insertion of the memory into the information system; and (ii) there are reliable hardware protections against reprogramming the memory while installed in organizational information systems. Related controls: AC-3, SI-7.	(1) NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE The organization employs [Assignment: organization-defined information system components] with no writeable storage that is persistent across component restart or power on/off. Supplemental Guidance: This control enhancement: (i) eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system components; and (ii) applies to both fixed and removable storage, with the latter being addressed directly or as specific restrictions imposed through access controls for mobile devices. Related controls: AC-19, MP-7. (2) NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA The organization protects the integrity of information prior to storage on read-only media and controls the media after such information has been recorded onto the media. Supplemental Guidance: Security safeguards prevent the substitution of media into information systems or the reprogramming of programmable read-only media prior to installation into the systems. Security safeguards include, for example, a combination of prevention, detection, and response. Related controls: AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3. (3) NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION The organization: (a) Employs hardware-based, write-protect for [Assignment: organization-defined information system firmware components]; and (b) Implements specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.	None
SC-35 **HONEYCLIENTS**	The information system includes components that proactively seek to identify malicious websites and/or web-based malicious code.	None	Honeyclients differ from honeypots in that the components actively probe the Internet in search of malicious code (e.g., worms) contained on external websites. As with honeypots, honeyclients require some supporting isolation measures (e.g., virtualization) to ensure that any malicious code discovered during the search and subsequently executed does not infect organizational information systems. Related controls: SC-26, SC-44, SI-3, SI-4.	None	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SC-37 **OUT-OF-BAND CHANNELS**	The organization employs [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, information system components, or devices] to [Assignment: organization-defined individuals or information systems].	None	Out-of-band channels include, for example, local (nonnetwork) accesses to information systems, network paths physically separate from network paths used for operational traffic, or nonelectronic paths such as the US Postal Service. This is in contrast with using the same channels (i.e., in-band channels) that carry routine operational traffic. Out-of-band channels do not have the same vulnerability/exposure as in-band channels, and hence the confidentiality, integrity, or availability compromises of in-band channels will not compromise the out-of-band channels. Organizations may employ out-of-band channels in the delivery or transmission of many organizational items including, for example, identifiers/authenticators, configuration management changes for hardware, firmware, or software, cryptographic key management information, security updates, system/data backups, maintenance information, and malicious code protection updates. Related controls: AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.	(1) OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION The organization employs [Assignment: organization-defined security safeguards] to ensure that only [Assignment: organization-defined individuals or information systems] receive the [Assignment: organization-defined information, information system components, or devices]. Supplemental Guidance: Techniques and/or methods employed by organizations to ensure that only designated information systems or individuals receive particular information, system components, or devices include, for example, sending authenticators via courier service but requiring recipients to show some form of government-issued photographic identification as a condition of receipt.	None
SC-40 **WIRELESS LINK PROTECTION**	The information system protects external and internal [Assignment: organization-defined wireless links] from [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].	None	This control applies to internal and external wireless communication links that may be visible to individuals who are not authorized information system users. Adversaries can exploit the signal parameters of wireless links if such links are not adequately protected. There are many ways to exploit the signal parameters of wireless links to gain intelligence, deny service, or to spoof users of organizational information systems. This control reduces the impact of attacks that are unique to wireless systems. If organizations rely on commercial service providers for transmission services as commodity items rather than as fully dedicated services, it may not be possible to implement this control. Related controls: AC-18, SC-5.	(1) WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE The information system implements cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference. Supplemental Guidance: This control enhancement protects against intentional jamming that might deny or impair communications by ensuring that wireless spread spectrum waveforms used to provide anti-jam protection are not predictable by unauthorized individuals. The control enhancement may also coincidentally help to mitigate the effects of unintentional jamming due to interference from legitimate transmitters sharing the same spectrum. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine levels of wireless link availability and performance/cryptography needed. Related controls: SC-12, SC-13. (2) WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL The information system implements cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction]. Supplemental Guidance: This control enhancement is needed for covert communications and protecting wireless transmitters from being geo-located by their transmissions. The control enhancement ensures that spread spectrum waveforms used to achieve low probability of detection are not predictable by unauthorized individuals. Mission requirements, projected threats, concept of operations, and applicable legislation, directives, regulations, policies, standards, and guidelines determine the levels to which wireless links should be undetectable. Related controls: SC-12, SC-13. (3) WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION The information system implements cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters. Supplemental Guidance: This control enhancement ensures that the signal parameters of wireless transmissions are not predictable by unauthorized individuals. Such unpredictability reduces the probability of imitative or manipulative communications deception based upon signal parameters alone. Related controls: SC-12, SC-13. (4) WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION The information system implements cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters. Supplemental Guidance: Radio fingerprinting techniques identify the unique signal parameters of transmitters to fingerprint such transmitters for purposes of tracking and mission/user identification. This control enhancement protects against the unique identification of wireless transmitters for purposes of intelligence exploitation by ensuring that anti-fingerprinting alterations to signal parameters are not predictable by unauthorized individuals. This control enhancement helps assure mission success when anonymity is required. Related controls: SC-12, SC-13.	None
SC-41 **PORT AND I/O DEVICE ACCESS**	The organization physically disables or removes [Assignment: organization-defined connection ports or input/output devices] on [Assignment: organization-defined information systems or information system components].	None	Connection ports include, for example, Universal Serial Bus (USB) and Firewire (IEEE 1394). Input/output (I/O) devices include, for example, Compact Disk (CD) and Digital Video Disk (DVD) drives. Physically disabling or removing such connection ports and I/O devices helps prevent exfiltration of information from information systems and the introduction of malicious code into systems from those ports/devices.	None	None
SC-42 **SENSOR CAPABILITY AND DATA**	The information system: a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and b. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].	None	This control often applies to types of information systems or system components characterized as mobile devices, for example, smart phones, tablets, and E-readers. These systems often include sensors that can collect and record data regarding the environment where the system is in use. Sensors that are embedded within mobile devices include, for example, cameras, microphones, Global Positioning System (GPS) mechanisms, and accelerometers. While the sensors on mobiles devices provide an important function, if activated covertly, such devices can potentially provide a means for adversaries to learn valuable information about individuals and organizations. For example, remotely activating the GPS function on a mobile device could provide an adversary with the ability to track the specific movements of an individual.	(1) SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES The organization ensures that the information system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles. Supplemental Guidance: In situations where sensors are activated by authorized individuals (e.g., end users), it is still possible that the data/information collected by the sensors will be sent to unauthorized entities. (2) SENSOR CAPABILITY AND DATA | AUTHORIZED USE The organization employs the following measures: [Assignment: organization-defined measures], so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes. Supplemental Guidance: Information collected by sensors for a specific authorized purpose potentially could be misused for some unauthorized purpose. For example, GPS sensors that are used to support traffic navigation could be misused to track movements of individuals. Measures to mitigate such activities include, for example, additional training to ensure that authorized parties do not abuse their authority, or (in the case where sensor data/information is maintained by external parties) contractual restrictions on the use of the data/information. (3) SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES The organization prohibits the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems]. Supplemental Guidance: For example, organizations may prohibit individuals from bringing cell phones or digital cameras into certain facilities or specific controlled areas within facilities where classified information is stored or sensitive conversations are taking place.	None
SC-43 **USAGE RESTRICTIONS**	The organization: a. Establishes usage restrictions and implementation guidance for [Assignment: organization-defined information system components] based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of such components within the information system.	None	Information system components include hardware, software, or firmware components (e.g., Voice Over Internet Protocol, mobile code, digital copiers, printers, scanners, optical devices, wireless technologies, mobile devices). Related controls: CM-6, SC-7.	None	None
SC-44 **DETONATION CHAMBERS**	The organization employs a detonation chamber capability within [Assignment: organization-defined information system, system component, or location].	None	Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted or suspicious applications, and execute Universal Resource Locator (URL) requests in the safety of an isolated environment or virtualized sandbox. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malicious code. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malicious code and reduce the likelihood that the code is propagated to user environments of operation (or prevent such propagation completely). Related controls: SC-7, SC-25, SC-26, SC-30.	None	None
SI-1 **SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**	The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency].	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the SI family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.	None	None
SI-2 **FLAW REMEDIATION**	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3	Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security-relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.	(1) FLAW REMEDIATION | CENTRAL MANAGEMENT The organization centrally manages the flaw remediation process. Supplemental Guidance: Central management is the organization-wide management and implementation of flaw remediation processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw remediation security controls. (2) FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS The organization employs automated mechanisms [Assignment: organization-defined frequency] to determine the state of information system components with regard to flaw remediation. Supplemental Guidance: Related controls: CM-6, SI-4. (3) FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS The organization: (a) Measures the time between flaw identification and flaw remediation; and (b) Establishes [Assignment: organization-defined benchmarks] for taking corrective actions. Supplemental Guidance: This control enhancement requires organizations to determine the current time it takes on the average to correct information system flaws after such flaws have been identified, and subsequently establish organizational benchmarks (i.e., time frames) for taking corrective actions. Benchmarks can be established by type of flaw and/or severity of the potential vulnerability if the flaw can be exploited. (4) FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS [Withdrawn: Incorporated into SI-2]. (5) FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES The organization installs [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined information system components]. Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Organizations must balance the need to ensure that the updates are installed as soon as possible with the need to maintain configuration management and with any mission or operational impacts that automatic updates might impose. (6) FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE The organization removes [Assignment: organization-defined software and firmware components] after updated versions have been installed. Supplemental Guidance: Previous versions of software and/or firmware components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software and/or firmware automatically from the information system.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SI-3 **MALICIOUS CODE PROTECTION**	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	A.12.2.1	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.	(1) MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT The organization centrally manages malicious code protection mechanisms. Supplemental Guidance: Central management is the organization-wide management and implementation of malicious code protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed flaw malicious code protection security controls. Related controls: AU-2, SI-8. (2) MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES The information system automatically updates malicious code protection mechanisms. Supplemental Guidance: Malicious code protection mechanisms include, for example, signature definitions. Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates. Related control: SI-8. (3) MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS [Withdrawn: Incorporated into AC-6 (10)]. (4) MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS The information system updates malicious code protection mechanisms only when directed by a privileged user. Supplemental Guidance: This control enhancement may be appropriate for situations where for reasons of security or operational continuity, updates are only applied when selected/approved by designated organizational personnel. Related controls: AC-6, CM-5. (5) MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES [Withdrawn: Incorporated into MP-7]. (6) MALICIOUS CODE PROTECTION | TESTING / VERIFICATION The organization: (a) Tests malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing a known benign, non-spreading test case into the information system; and (b) Verifies that both detection of the test case and associated incident reporting occur. Supplemental Guidance: Related controls: CA-2, CA-7, RA-5. (7) MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION The information system implements nonsignature-based malicious code detection mechanisms. Supplemental Guidance: Nonsignature-based detection mechanisms include, for example, the use of heuristics to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against malicious code for which signatures do not yet exist or for which existing signatures may not be effective. This includes polymorphic malicious code (i.e., code that changes signatures when it replicates). This control enhancement does not preclude the use of signature-based detection mechanisms. (8) MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS The information system detects [Assignment: organization-defined unauthorized operating system commands] through the kernel application programming interface at [Assignment: organization-defined information system hardware components] and [Selection (one or more): issues a warning; audits the command execution; prevents the execution of the command]. Supplemental Guidance: This control enhancement can also be applied to critical interfaces other than kernel-based interfaces, including for example, interfaces with virtual machines and privileged applications. Unauthorized operating system commands include, for example, commands for kernel functions from information system processes that are not trusted to initiate such commands, or commands for kernel functions that are suspicious even though commands of that type are reasonable for processes to initiate. Organizations can define the malicious commands to be detected by a combination of command types, command classes, or specific instances of commands. Organizations can define hardware components by specific component, component type, location in the network, or combination therein. Organizations may select different actions for different types/classes/specific instances of potentially malicious commands. Related control: AU-6. (9) MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS The information system implements [Assignment: organization-defined security safeguards] to authenticate [Assignment: organization-defined remote commands].	None
SI-4 **INFORMATION SYSTEM MONITORING**	The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].	None	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.	(1) INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system. (2) INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS The organization employs automated tools to support near real-time analysis of events. Supplemental Guidance: Automated tools include, for example, host-based, network-based, transport-based, or storage-based event monitoring tools or Security Information and Event Management (SIEM) technologies that provide real time analysis of alerts and/or notifications generated by organizational information systems. (3) INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (4) INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC The information system monitors inbound and outbound communications traffic [Assignment: organization-defined frequency] for unusual or unauthorized activities or conditions. Supplemental Guidance: Unusual/unauthorized activities or conditions related to information system inbound and outbound communications traffic include, for example, internal traffic that indicates the presence of malicious code within organizational information systems or signaling to external information systems. Evidence of malicious code is used to identify potentially compromised information systems or information system components. (5) INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators]. Supplemental Guidance: Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system owners, or information system security officers. Related controls: AU-5, PE-6. (6) INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS [Withdrawn: Incorporated into AC-6 (10)]. (7) INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS The information system notifies [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events and takes [Assignment: organization-defined least-disruptive actions to terminate suspicious events]. Supplemental Guidance: Least-disruptive actions may include, for example, initiating requests for human responses. (8) INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION [Withdrawn: Incorporated into SI-4]. (9) INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS The organization tests intrusion-monitoring tools [Assignment: organization-defined frequency]. Supplemental Guidance: Testing intrusion-monitoring tools is necessary to ensure that the tools are operating correctly and continue to meet the monitoring objectives of organizations. The frequency of testing depends on the types of tools used by organizations and methods of deployment. Related control: CP-9. (10) INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS The organization makes provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined information system monitoring tools]. Supplemental Guidance: Organizations balance the potentially conflicting needs for encrypting communications traffic and for having insight into such traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of communications traffic is paramount; for others, mission-assurance is of greater concern. Organizations determine whether the visibility requirement applies to internal encrypted traffic,	None
SI-5 **SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**	The organization: a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	A.6.1.4 (only partially satisfies NIST control)	The United States Computer Emergency Readiness Team (US-CERT) generates security alerts and advisories to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse effects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. External organizations include, for example, external mission/business partners, supply chain partners, external service providers, and other peer/supporting organizations. Related control: SI-2.	(1) SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES The organization employs automated mechanisms to make security alert and advisory information available throughout the organization. Supplemental Guidance: The significant number of changes to organizational information systems and the environments in which those systems operate requires the dissemination of security-related information to a variety of organizational entities that have a direct interest in the success of organizational missions and business functions. Based on the information provided by the security alerts and advisories, changes may be required at one or more of the three tiers related to the management of information security risk including the governance level, mission/business process/enterprise architecture level, and the information system level.	None
SI-6 **SECURITY FUNCTION VERIFICATION**	The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.	None	Transitional states for information systems include, for example, system startup, restart, shutdown, and abort. Notifications provided by information systems include, for example, electronic alerts to system administrators, messages to local computer consoles, and/or hardware indications such as lights. Related controls: CA-7, CM-6.	(1) SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS [Withdrawn: Incorporated into SI-6]. (2) SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING The information system implements automated mechanisms to support the management of distributed security testing. Supplemental Guidance: Related control: SI-2. (3) SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS The organization reports the results of security function verification to [Assignment: organization-defined personnel or roles]. Supplemental Guidance: Organizational personnel with potential interest in security function verification results include, for example, senior information security officers, information system security managers, and information systems security officers. Related controls: SA-12, SI-4, SI-5.	None

Control (NIST SP 800-53, r4)	**Control Specifics** (SP 800-53, r4)	**ISO/IEC 27001 Controls that fulfill the NIST Control** (SP 800-53, r4, Appendix H)	**Supplemental Guidance** (SP 800-53, r4)	**Control Enhancements** (SP 800-53, r4)	**Additional Stryker Guidance for Control**
SI-7 **SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**	The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].	None	Unauthorized changes to software, firmware, and information can occur due to errors or malicious activity (e.g., tampering). Software includes, for example, operating systems (with key internal components such as kernels, drivers), middleware, and applications. Firmware includes, for example, the Basic Input Output System (BIOS). Information includes metadata such as security attributes associated with information. State-of-the-practice integrity-checking mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of information systems and hosted applications. Related controls: SA-12, SC-8, SC-13, SI-3.	(1) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]]. Supplemental Guidance: Security-relevant events include, for example, the identification of a new threat to which organizational information systems are susceptible, and the installation of new hardware, software, or firmware. Transitional states include, for example, system startup, restart, shutdown, and abort. (2) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification. Supplemental Guidance: The use of automated tools to report integrity violations and to notify organizational personnel in a timely matter is an essential precursor to effective risk response. Personnel having an interest in integrity violations include, for example, mission/business owners, information system owners, systems administrators, software developers, systems integrators, and information security officers. (3) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY-MANAGED INTEGRITY TOOLS The organization employs centrally managed integrity verification tools. Supplemental Guidance: Related controls: AU-3, SI-2, SI-8. (4) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING [Withdrawn: Incorporated into SA-12]. (5) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered. Supplemental Guidance: Organizations may define different integrity checking and anomaly responses: (i) by type of information (e.g., firmware, software, user data); (ii) by specific information (e.g., boot firmware, boot firmware for a specific types of machines); or (iii) a combination of both. Automatic implementation of specific safeguards within organizational information systems includes, for example, reversing the changes, halting the information system, or triggering audit alerts when unauthorized modifications to critical security files occur. (6) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to detect unauthorized changes to software, firmware, and information. Supplemental Guidance: Cryptographic mechanisms used for the protection of integrity include, for example, digital signatures and the computation and application of signed hashes using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information. Related control: SC-13. (7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability. Supplemental Guidance: This control enhancement helps to ensure that detected events are tracked, monitored, corrected, and available for historical purposes. Maintaining historical records is important both for being able to identify and discern adversary actions over an extended period of time and for possible legal actions. Security-relevant changes include, for example, unauthorized changes to established configuration settings or unauthorized elevation of information system privileges. Related controls: IR-4, IR-5, SI-4. (8) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS The information system, upon detection of a potential integrity violation, provides the capability to audit the event and initiates the following actions: [Selection (one or more): generates an audit record; alerts current user; alerts [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]]. Supplemental Guidance: Organizations select response actions based on types of software, specific software, or information for which there are potential integrity violations. Related controls: AU-2, AU-6, AU-12. (9) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS The information system verifies the integrity of the boot process of [Assignment: organization-defined devices].	None
SI-8 **SPAM PROTECTION**	The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.	None	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, mobile devices, and notebook/laptop computers. Spam can be transported by different means including, for example, electronic mail, electronic mail attachments, and web accesses. Spam protection mechanisms include, for example, signature definitions. Related controls: AT-2, AT-3, SC-5, SC-7, SI-3.	(1) SPAM PROTECTION | CENTRAL MANAGEMENT The organization centrally manages spam protection mechanisms. Supplemental Guidance: Central management is the organization-wide management and implementation of spam protection mechanisms. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed spam protection security controls. Related controls: AU-3, SI-2, SI-7. (2) SPAM PROTECTION | AUTOMATIC UPDATES The information system automatically updates spam protection mechanisms. (3) SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY The information system implements spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic. Supplemental Guidance: Learning mechanisms include, for example, Bayesian filters that respond to user inputs identifying specific traffic as spam or legitimate by updating algorithm parameters and thereby more accurately separating types of traffic.	None
SI-10 **INFORMATION INPUT VALIDATION**	The information system checks the validity of [Assignment: organization-defined information inputs].	None	Checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content. Software applications typically follow well-defined protocols that use structured messages (i.e., commands or queries) to communicate between software modules or system components. Structured messages can contain raw or unstructured data interspersed with metadata or control information. If software applications use attacker-supplied inputs to construct structured messages without properly encoding such messages, then the attacker could insert malicious commands or special characters that can cause the data to be interpreted as control information or metadata. Consequently, the module or component that receives the tainted output will perform the wrong operations or otherwise interpret the data incorrectly. Prescreening inputs prior to passing to interpreters prevents the content from being unintentionally interpreted as commands. Input validation helps to ensure accurate and correct inputs and prevent attacks such as cross-site scripting and a variety of injection attacks.	(1) INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY The information system: (a) Provides a manual override capability for input validation of [Assignment: organization-defined inputs]; (b) Restricts the use of the manual override capability to only [Assignment: organization-defined authorized individuals]; and (c) Audits the use of the manual override capability. Supplemental Guidance: Related controls: CM-3, CM-5. (2) INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS The organization ensures that input validation errors are reviewed and resolved within [Assignment: organization-defined time period]. Supplemental Guidance: Resolution of input validation errors includes, for example, correcting systemic causes of errors and resubmitting transactions with corrected input. (3) INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR The information system behaves in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received. Supplemental Guidance: A common vulnerability in organizational information systems is unpredictable behavior when invalid inputs are received. This control enhancement ensures that there is predictable behavior in the face of invalid inputs by specifying information system responses that facilitate transitioning the system to known states without adverse, unintended side effects. (4) INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS The organization accounts for timing interactions among information system components in determining appropriate responses for invalid inputs. Supplemental Guidance: In addressing invalid information system inputs received across protocol interfaces, timing interactions become relevant, where one protocol needs to consider the impact of the error response on other protocols within the protocol stack. For example, 802.11 standard wireless network protocols do not interact well with Transmission Control Protocols (TCP) when packets are dropped (which could be due to invalid packet input). TCP assumes packet losses are due to congestion, while packets lost over 802.11 links are typically dropped due to collisions or noise on the link. If TCP makes a congestion response, it takes precisely the wrong action in response to a collision event. Adversaries may be able to use apparently acceptable individual behaviors of the protocols in concert to achieve adverse effects through suitable construction of invalid input. (5) INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS The organization restricts the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats]. Supplemental Guidance: This control enhancement applies the concept of whitelisting to information inputs. Specifying known trusted sources for information inputs and acceptable formats for such inputs can reduce the probability of malicious activity.	None
SI-11 **ERROR HANDLING**	The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defined personnel or roles].	None	Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information such as account numbers, social security numbers, and credit card numbers. In addition, error messages may provide a covert channel for transmitting information. Related controls: AU-2, AU-3, SC-31.	None	None
SI-12 **INFORMATION HANDLING AND RETENTION**	The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	None	Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems. The National Archives and Records Administration provides guidance on records retention. Related controls: AC-16, AU-5, AU-11, MP-2, MP-4.	None	None
SI-15 **INFORMATION OUTPUT FILTERING**	The information system validates information output from [Assignment: organization-defined software programs and/or applications] to ensure that the information is consistent with the expected content.	None	Certain types of cyber attacks (e.g., SQL injections) produce output results that are unexpected or inconsistent with the output results that would normally be expected from software programs or applications. This control enhancement focuses on detecting extraneous content, preventing such extraneous content from being displayed, and alerting monitoring tools that anomalous behavior has been discovered. Related controls: SI-3, SI-4.	None	None
SI-17 **FAIL-SAFE PROCEDURES**	The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].	None	Failure conditions include, for example, loss of communications among critical system components or between system components and operational facilities. Fail-safe procedures include, for example, alerting operator personnel and providing specific instructions on subsequent steps to take (e.g., do nothing, reestablish system settings, shut down processes, restart the system, or contact designated organizational personnel). Related controls: CP-12, CP-13, SC-24, SI-13.	None	None

PRODUCT SECURITY STANDARD ASSESSMENT - Privacy by Design (PbD) Baseline Requirements			
Definition of key privacy terms and additional Privacy by Design explanations may be located in D0000061607, Privacy by Design.			
PbD Family and Purpose	**PbD Sub-element and Purpose**	**PbD Control**	**PbD Baseline Requirements**
1. Authority & Purpose This family ensures that organizations: (i) identify the legal bases that authorize a particular personal information (PI) collection or activity that impacts privacy; and (ii) specify in their notices the purpose(s) for which PI is collected.	**1.1 Authority to collect** Specification of Controller/Processor (GDPR), Covered Entity/Business Associate (HIPAA), consent, data flows	**1.1.1 Authority to collect in GDPR**	(1) When SYK is a controller, determine the Legal basis (IP-1 Consent from NIST SP 800-53, or any other) and provide a Privacy notice to the data subject (TR-1 Privacy Notice from NIST SP 800-53). If there are data exchanges with other parties, appropriate Data Processing Agreements between SYK and those parties shall be established. (1.a.) When SYK is a joint controller together with another party, create appropriate Joint Controller Agreements between Stryker and other party regarding the responsibilities for the PI flowing through the device. (1.b.) When SYK is a controller in common with another controller, no Data Processing Agreement is required as they operate as separate parties. (1.c.) In all above cases legal or compliance shall be contacted for further advise. (2.) When SYK is a processor on behalf of a hospital, create appropriate Data Processing Agreements between Stryker and Customer regarding the responsibilities for the PI flowing through the device. (2.a.) When SYK is a sub-processor on behalf of another party, ensure activities are aligned with data protection standard agreed in Contractual Agreements between Controller and Processor.
		1.1.2 Authority to collect in HIPAA	(1) When SYK is a covered entity (very unlikely) contact legal in order to clarify specific requirements. (2) When SYK is a business associate establish a Business Associate Agreement.
		1.1.3 Authority to collect in architectural diagrams	(1) A system architecture visual shall depict the data flow of privacy data through major components and interfaces of the device. (2) An architectural context diagram shall depict how the device will be embedded in a customer environment and how the above defined roles apply in this device application context. (3) The system architecture visual and the architectural context diagram shall also be documented in the Security Operations Manual (SOM) for customer information reasons without disclosing proprietary information.
	1.2 Purpose specification Personal data may only be collected for specified, explicit and legitimate purposes. Define purpose of collection. Ensure data flow structure supports only defined purpose.	**1.2.1 Purpose specification in architectural diagrams**	The main purpose shall be explicitly defined in an architectural document.
		1.2.2 Purpose limitation	The data and functional structure of the device shall guarantee the purpose limitations and shall not allow the system to be used outside the scope of the purpose definition. This means that the personal information acquired and kept by the device shall be restricted to information which is necessary to fulfill the stated purpose.
		1.2.3 Purpose definition in SOM	The purpose definition shall be documented in the Security Operations Manual (SOM).
2. Accountability, Audit, Risk Management This family enhances public confidence through effective controls for governance, monitoring, risk management, and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.	**2.1 Governance & Privacy Program** Senior roles are appointed to safeguard Privacy & Security	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
	2.2 Privacy Impact & Risk Assessment Standard methods are used to conduct risk assessments & mitigate risk	**2.2.1 Data Privacy Impact Assessment**	A (Data) Privacy Impact Assessment (DPIA) shall be performed. The outcome of the privacy impact assessment may need to be considered in (a) the security risk assessment, or (b) any other design output documentation for further specification of data protection controls.
	2.3 Privacy Requirements for Contractors and Service Providers Contracts are used to establish requirements for contractors and providers	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
	2.4 Privacy Monitoring and Auditing Auditing program defines responsibilities	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
	2.5 Privacy Awareness & Training The workforce is trained on the requirements	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
	2.6 Privacy Reporting Reporting to senior management, and to authorities where required	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
	2.7 Privacy Enhanced System Design & Development Use of access controls, anonymization, pseudonymization, and/or encryption	**2.7.1 Data minimization**	Use the least amount of Personal information in order to fulfill the defined purpose and control access based on 'need to know' and/or roles and responsibilities. Consider the use of independent certified partners to verify.
		2.7.2 Pseudonymization	Ensure with appropriate techniques that critical (health) information cannot be related to its related individual without additional information. Consider the use of independent certified partners to verify.
		2.7.3 Anonymization	Ensure with appropriate techniques and in a statistical valid manner that critical (health) information cannot be related to its related individual in any way. Consider the use of independent certified partners to verify.

PbD Family and Purpose	PbD Sub-element and Purpose	PbD Control	PbD Baseline Requirements
		2.7.4 Encryption	Ensure that data at rest and data in transition is encrypted. Consider the use of independent certified partners to verify.
	2.8 Accounting of Disclosure Use of data inventory, registration of disclosures	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
3. Data Quality & Integrity This family enhances public confidence that any personally identifiable information (PI) collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.	**3.1 Data Quality** Ensure mechanisms exist to keep data up to date, discover mistaken data and have the ability to correct data.	**3.1.1 Data Quality Mechanism**	A mechanism shall ensure that data is kept up to date, discover mistaken data, and have the ability to correct data.
		3.1.2 Data integrity in the SOM	The Security Operations Manual (SOM) shall contain appropriate instructions when customer involvement is needed to maintain data integrity.
	3.2 Data Integrity & Data Integrity Board Establish methods to ensure confidentiality, integrity and availability of personal information and flags for vulnerabilities	**3.2.1 Additional Data Processing Functions for Integrity**	In order to maintain the integrity of PI, suitable data processing functionality may be considered. For instance, an automatic audit function can be used to flag relevant changes to data or other specific requirements of "Electronic Code of Federal Regulations, Part 11" may apply.
4. Data Minimization & Retention This family helps organizations implement the data minimization and retention requirements to collect, use, and retain only personal information (PI) that is relevant and necessary for the purpose for which it was originally collected. Organizations retain PI for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with approved record retention schedules.	**4.1 Minimization of personally identifiable Information** Collect only minimal amount of data	This sub-element requires that the device is designed so the it only acquires and keeps personal information to the extent that is needed to fulfill the purpose outlined in the purpose specification, and requires the purpose definition to be documented in the SOM. Since these requirements are already stated in 1.2.2 and 1.2.3 above, they do not need to be assessed again within family 4.1.	
	4.2 Data Retention and Disposal Only keep data for duration required by law and as needed for the purpose; delete afterward	**4.2.1 Enabling deletion of data**	Include functionality that allows data deletion to ensure that data is not kept longer than defined in the purpose specification.
		4.2.2 Time Stamp Identification	Mark personal data with time stamp information to enable it to be selected for deletion on the basis of when it was acquired or stored.
		4.2.3 Data Disposal in SOM	Include a statement in the Security Operations Manual (SOM) to ensure that the customer follows applicable data minimization rules and to explain how data my be deleted.
	4.3 Minimization of PII used in Testing, Training, and IP Use of minimal identifiable data for testing	**4.3.1 Use of Dummy Data for Testing**	When test data is needed, dummy data shall be specified and used instead of personal data from real persons. This may consist of de-identified data or 'fake' data not derived from real personal data.
5. Individual Participation & Redress This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their personally identifiable information (PII). By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.	**5.1 Consent** If Stryker acts as a controller and collects PHI, consent from individuals may be necessary	**5.1.1 Consent if Controller**	If Stryker is defined as data controller for this product, consider setting up the workflow such that a patient consent degree is required before any data processing starts.
		5.1.2 Consent if Processor	If Stryker is defined as data processor for this product, consider adding a warning statement on the device with a message similar to, "This product processes personal data. The surgeon is responsible for obtaining patient consent for product use when appropriate."
	5.2 Individual Access Responding to individuals' requests for access to their PI	**5.2.1 Functionality for Individual Data Access Requests**	The device shall be able to support requests of individuals for access to their Personal Information. Note: Patients do not need to get access to the device. A machine-readable (soft copy) export summary (pdf) could satisfy this requirement. Ensure that PI from others is redacted.
	5.3 Redress Responding to individuals' requests for deletion, restriction, revision, etc. of their PI	**5.3.1 Functionality for Individual Data Activity Requests**	The device shall be able to support requests of individuals for deletion, restriction of processing, revision or portability of their Personal Information. Note: Patients do not need to get access to the device or be able to perform the modifications themselves. A confirmation of deletion, continued restricted use, revision/correction of data or portable copy could satisfy this requirement.
	5.4 Complaint or request management Responding to complaints and general requests	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
6. Security This family supplements the security controls to ensure that technical, physical, and administrative safeguards are in place to protect personally identifiable information (PII) collected or maintained by organizations against loss,	**6.1 Inventory of Personally Identifiable Information** Data Inventory, Data Flows, Product Lifecycle Overview, Contracts	This sub-element's requirements are covered by the architectural and data flow requirements in sub-element 1.2 Purpose Specification.	

PbD Family and Purpose	PbD Sub-element and Purpose	PbD Control	PbD Baseline Requirements
unauthorized access, or disclosure, and to ensure that planning and responses to privacy incidents comply with security regulations worldwide. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing Risk Management Framework.	**6.2 Privacy Incident Response** Incident response plans, breach notification assessment and methods	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
7. Transparency This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.	**7.1 Privacy Notice** Where Stryker is a data controller (GDPR) it needs to inform individuals about its PI collection and privacy practices through a privacy statement	**7.1.1 Transparency if Controller**	If Stryker is defined as data controller for this product, consider setting up the workflow such that a patient is informed about the data collection before any data processing starts.
	7.2 System of Records Any Privacy Notices and declared data inventories to authorities should be kept up to date	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
	7.3 Dissemination of Privacy program information Materials should be developed and disseminated in the organization which demonstrate accountable privacy practices, including a Privacy Policy	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	
8. Use Limitation This family ensures that organizations only use personal information (PI) either as specified in their public notices, in a manner compatible with those specified purposes, or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PI use is limited accordingly.	**8.1 Internal Use** Internal Privacy Policy, in which data usage is aligned with privacy policy and privacy notices and is otherwise addressed, or updates made to privacy policy or privacy notices	**8.1.1 Internal Use Policies**	If Stryker is defined as data controller for this product, the legal or compliance department shall be contacted for further advice concerning internal use.
	8.2 Information Sharing with Third Parties Privacy policy and notices and contracts include information on information sharing practices	This sub-element has no baseline requirements for the design of individual products. It relates to systemic or orgnizational privacy requirements.	